uc3m | Universidad Carlos III de Madrid

TESIS DOCTORAL

La transparencia como elemento de apoyo al consentimiento en materia de Protección de Datos

Autor:

Juan Antonio Prego de Oliver Fernández

Director/es:

Agustín E. de Asís Roig

Tutor:

Agustín E. de Asís Roig

DERECHO PÚBLICO DEL ESTADO

Getafe, junio 2017

uc3m | Universidad Carlos III de Madrid

(a entregar en la Oficina de Postgrado, una vez nombrado el Tribunal evaluador, para preparar el documento para la defensa de tesis)

TESIS DOCTORAL

La transparencia como elemento de apoyo al consentimiento en materia de Protección de Datos

Autor: *(Juan Antonio Prego de Oliver Fernández)*

Director/es: **(Agustín E. de Asís Roig)**

Firma del Tribunal Calificador:

Firma

Presidente: (Nombre y apellidos)

Vocal: (Nombre y apellidos)

Secretario: (Nombre y apellidos)

Calificación:

Getafe, de de

TABLA DE ABREVIATURAS

- AEPD.- Agencia Española de Protección de Datos
- AGE.- Administración General del Estado.
- ARCO.- Acrónimo que hace referencia al derecho de acceso, al de rectificación, al de cancelación y al de oposición
- BEUC.- Asociación Europea de Consumidores.
- CE.- Constitución Española de 1978. BOE núm 311, de 29/12/1978.
- CEADP.- Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos. Tromsø, 18 de junio de 2009
- CEDH.- Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales
- DOCE.- Diario Oficial de las Comunidades Europeas
- DOUE.- Diario Oficial de la Unión Europea.
- EDPS.- Supervisor Europeo de Proteción de Datos
- EIPD.- Evaluación de Impacto en la Protección de Datos. En inglés se denomina PIA (Privacy Impact Assessment).
- FOIA.- Freedom of Information Act.
- GT29.- Grupo de Trabajo del Artículo 29.
- ICO.- Oficina del Comisionado de Información.
- INAP.- Instituto Nacional de las Administraciones Públicas
- LGTel.- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones. BOE núm 114, de 10/05/2014.
- LOPD.- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm 298, de 14/12/1999.
- LPACAP.- Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE núm 236, de 02/10/2015.
- LPHE.- Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. BOE núm 155, de 29/06/1985.
- LRJPAC .- Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. BOE núm 285, de 27/11/1992.

- LRJSP.- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. BOE núm 236, de 02/10/2015.
- LSSI.- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. BOE núm. 166, de 12/07/2002.
- LTBG.- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno. BOE núm 295, de 10/12/2013.
- OCDE.- Organización para la Cooperación y el Desarrollo Económicos.
- PbD.- Privacidad desde el diseño. Conocido así por sus siglas en inglés (Privacy by Design).
- PET.- Privacy Enhancing Technologies.
- pp.- Páginas.
- RAE.- Real Academia Española.
- RGPD. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) DOUE L 119 de 4.5.2016.
- RLOPD. Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. BOE núm, 17, de 19 de enero de 2008.
- STC.- Sentencia del Tribunal Constitucional.
- STS.- Sentencia del Tribunal Supremo.
- TCEE.- Tratado Constitutivo de la Comunidad Económica Europea. El Tratado de Roma se ha modificado en varias ocasiones, y actualmente se denomina Tratado de Funcionamiento de la Unión Europea. DOUE C 202, de 07 de junio de 2016.
- TEDH.- Tribunal Europeo de Derechos Humanos
- TIC.- Tecnologías de la Información y las Comunicaciones.
- TJUE.- Tribunal de Justicia de la Unión Europea.

– TUE.- Tratado de la Unión Europea. El Tratado de Maastricht ha sido modificado hasta en tres ocasiones, y en la actualidad se denomina Tratado de Lisboa. DOUE C 306, de 17 de diciembre de 2007.
– UE.- Unión Europea.

ÍNDICE

TABLA DE CONTENIDO

INTRODUCCIÓN

En los últimos años se produce una mayor demanda de conocimiento de la información pública y una mayor transparencia administrativa, lo que implica tanto un acceso por parte del ciudadano sin necesidad de acreditar un interés legítimo, como una publicación de información a iniciativa de las Administraciones Públicas. Así, se hace referencia, no solo a una solicitud de acceso por parte de ciudadano a información administrativa, sino a la obligación de la Administración de difundir de oficio una determinada información.

Expone TRONCOSO REIGADA[1] que esta demanda de transparencia administrativa estaría vinculada a aquellos movimientos que propugnan una democracia real, una toma del poder por parte de los ciudadanos, y una sociedad más participativa, que tienen como presupuesto el acceso a la información administrativa.

La transparencia es necesaria en muchas ocasiones para que la Administración Pública sirva con objetividad los intereses generales y actúe en cada uno de los procedimientos administrativos con imparcialidad y con sometimiento pleno a la ley y al Derecho[2]. De ese modo, el acceso a la información facilita el respeto de la Administración al principio de legalidad y la vinculación de los poderes públicos a los propios actos.

Conforme establece en el Preámbulo del Convenio del Consejo de Europa, de 27 de noviembre de 2008, sobre el Acceso a los Documentos Públicos,

---

[1] Troncoso Reigada, A. (2010). Transparencia administrativa y protección de datos personales. En Troncoso Reigada, A. *La protección de datos personales en busca del equilibrio*. Valencia: Tirant lo Blanch. p 702.

[2] Véase el artículo 103.1 CE al reconocer en su apartado 1 expresamente que «La Administración Pública sirve con objetividad los intereses generales y actúa de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho».

el derecho de acceso supone que «todos los documentos son en principio públicos, y solamente pueden ser retenidos para proteger otros derechos e intereses legítimos». Así, «cada parte garantizará el derecho de cualquiera, sin discriminación de ningún tipo a acceder, bajo petición, a los documentos públicos en posesión de las autoridades públicas»[3].

Ahora bien, esta igualdad en el acceso a la información pública no se proyecta únicamente en las relaciones con la Administración, sino que tiene consecuencias en las relaciones entre particulares. Nos encontramos también ante una demanda de la propia libertad de empresa y del funcionamiento transparente de la economía del mercado[4], que exige una sociedad abierta. Una manifestación de esto último se produce cuando la solicitud de acceso tiene como finalidad la reutilización con fines comerciales de información en poder de la Administración.

No obstante, el acceso a la información pública no es un derecho absoluto, sino que está sometido a límites que deben estar establecidos en una ley, ser legítimos y proporcionales. Entre estos límites, destacamos la protección de datos personales[5]. Por tanto, en ocasiones nos hallamos ante un difícil equilibrio entre los valores constitucionales que demandan una mayor publicidad de la información y aquellos otros que por el contrario exigen reserva.

Reconoce la doctrina[6] de forma común que

---

[3] Véase artículo 2.1 del Convenio del Consejo de Europa sobre Acceso a los Documentos Públicos, Tromsø, 18 de junio de 2009.

[4] Véase el artículo 38 CE, de cuyo tenor literal se afirma que «se reconoce la libertad de empresa en el marco de la economía de mercado. Los poderes públicos garantizan y protegen su ejercicio y la defensa de la productividad, de acuerdo con las exigencias de la economía general y, en su caso, de la planificación».

[5] Véanse los artículos 23 y 24 LOPD.

[6] Troncoso Reigada, A. (2010). Transparencia administrativa y protección de datos personales. En Troncoso Reigada, A. *La protección de datos personales en busca del equilibrio*. Valencia: Tirant lo Blanch. p 728.

«La información administrativa que afecte a la intimidad de las personas debe ser considerada confidencial. Igualmente, los ordenamientos jurídicos que reconocen el derecho de acceso a información administrativa pueden limitarlo cuando afecte a otros valores constitucionales, como son la seguridad nacional, la defensa del Estado, la prevención y la persecución de los delitos, las relaciones internacionales, las actuaciones administrativas en materia tributaria o que afecten a la estabilidad financiera, el secreto industrial y los intereses comerciales».

La necesidad de esta reserva se hace manifiestamente notorio cuando la petición de acceso recae sobre datos personales sometidos a tratamiento. Y es que, todos nuestros datos se encuentran en poder de la Administración, y un acceso indiscriminado a estos, puede suponer una transparencia absoluta por parte de los administrados.

Sin embargo, para que opere este límite, no es suficiente con la existencia de algún dato personal en la documentación administrativa que se solicita el acceso. Es necesario que exista un tratamiento de datos personales. Asimismo, no se puede afirmar que cualquier acceso a una documentación administrativa donde se encuentren datos personales sería una comunicación o cesión de datos personales. Si no existe un tratamiento, ya sea manual o informatizado, el derecho fundamental a la protección de datos personales no supone un límite. Este acceso, podría afectar al derecho a la privacidad, pero no a la protección de datos personales. Así, la protección de datos personales tiene un objeto y un ámbito de aplicación distinto al derecho a la intimidad o a la privacidad personal.

Reconoce TRONCOSO REIGADA que el derecho fundamental a la protección de datos personales representa un límite a la publicación de datos personales, ya que la publicación supone un tratamiento de información, una cesión indiscriminada[7] de datos personales sin cesionario

[7] La definición de tratamiento de datos aparece reflejada en el apartado h) del artículo 3 LOPD en los siguientes términos: «A los efectos de la presente Ley Orgánica se entenderá por: […] c) Tratamiento de datos: operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la

conocido»[8]. La publicación de datos personales es un tratamiento masivo, hace que el ciudadano pierda el control de su información personal. Deja de saber quién tiene sus datos y para qué finalidad.

De igual modo, es habitual calificar la sociedad actual como sociedad del conocimiento, destacando así el papel central que ha asumido la información, especialmente como consecuencia del desarrollo de las tecnologías de la información y del conocimiento.

Es también una sociedad del reciclaje, caracterizada por la creciente tendencia a reutilizar, ya sea por motivos medioambientales o estrictamente económicos, unos recursos habitualmente escasos[9]. Entre estos, se encuentra la información que tiene un valor económico nada despreciable.

Como consecuencia de su actividad, las administraciones públicas disponen de un gran volumen de información, mucha de ella valiosa en el mercado.

Tradicionalmente, la reutilización de la información del sector público ha sido realizada por el sector privado que, en base a la información en bruto que recibía de las administraciones públicas, la trataba, la reelaboraba, a editaba y la ponía a disposición de los consumidores. Las administraciones públicas eran los productores de información que debían ponerla a disposición del sector privado encargado de su presentación y su posterior difusión y comercialización.

Sin embargo, en los últimos años, la información del sector público, no es vista únicamente como un elemento indispensable para el desarrollo de su actividad administrativa. También es considerada como un importante activo

---

recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias».

[8] Troncoso Reigada, A. (2010). Transparencia administrativa y protección de datos personales. En Troncoso Reigada, A. *La protección de datos personales en busca del equilibrio*. Valencia: Tirant lo Blanch. p 739.

[9] Cerrillo i Martínez, A. (2006). La información del sector público: del acceso a la reutilización. En Cerrillo Martínez, A. y Galán Galán, A. (Coord.), *La reutilización de la información del sector público*. Granada: Comares.

cuya reutilización por parte de empresas privadas puede impulsar la actividad económica y la creación de riqueza. La reutilización de información pública está principalmente orientada a fomentar la economía de mercado, valorando los datos que dispone la Administración como un importante activo económico, como materia prima para nuevos productos y servicios digitales.

El uso de las tecnologías de la información y la comunicación por las administraciones públicas ha facilitado la difusión de la información del sector público y su conocimiento por los ciudadanos y las empresas. Pero, además, ha facilitado su reutilización para finalidades diferentes de las que fue originalmente producida. En particular, la explotación comercial.

Señala CERRILLO i MARTÍNEZ que la economía digital basada en el conocimiento tiene un fuerte impacto en la vida de todos los europeos y puede convertirse en un motor de crecimiento, competitividad y empleo, al tiempo que mejora la calidad de vida de los ciudadanos. Un mejor acceso y utilización de esta información constituiría un valioso activo para los ciudadanos, las empresas y las administraciones. Las tecnologías de la información y la comunicación han potenciado este papel de la información como motor de desarrollo, y están ampliando enormemente la información en poder de los ciudadanos y diversificando de forma importante, tanto cuantitativa como, especialmente, cualitativamente, los mecanismos de gestión y transmisión de la información; lo que está incidiendo de manera importante en los diferentes usos que se dan a la información del sector público. Los ciudadanos y las empresas podrán extraer un enorme beneficio de la disponibilidad de información del sector público a través de Internet. Con ello se facilitará su comunicación con las administraciones públicas y se les ofrecerá una posibilidad de incrementar su participación en el proceso

democrático. La información del sector público es un activo económico y una mercancía en potencia[10].

Tal es así, que ha dado lugar a promulgar normativa europea, y por ende, en nuestro país, normativa nacional[11]. Es en esta última donde encontramos la definición del término «reutilización». Así, el artículo 3.1 de la Ley 37/2007, declara:

> *«Se entiende por reutilización el uso de documentos que obran en poder de las Administraciones y organismos del sector público, por personas físicas o jurídicas, con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública. Queda excluido de este concepto el intercambio de documentos entre Administraciones y organismos del sector público en el ejercicio de las funciones públicas que tengan atribuidas».*

Ahora bien, este planteamiento quedaría limitado si no apuntáramos brevemente los graves problemas que se plantean con el uso de la reutilización de la información de los poderes públicos, por parte del sector privado. Problemas de muy diversa índole, viéndose afectados tanto la competencia en el mercado, como el principio de calidad de los datos, pasando por la propiedad intelectual.

En un primero lugar, todo esto ha sido visto con gran recelo por las empresas de contenidos al considerar que la comercialización de la información del

---

[10] Cerrillo i Martínez, A. (2006). La información del sector público: del acceso a la reutilización. En Cerrillo Martínez, A. y Galán Galán, A. (Coord.), *La reutilización de la información del sector público*. Granada: Comares

[11] En este sentido, en Europa se aprueba la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre, relativa a la reutilización de la información del sector público [DOUE L 345 de 31 de diciembre de 2003], modificada por la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público [DOUE L 175 de 27 de junio de 2013]. En idéntico sentido, en España se aprueba la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (BOE núm 276, de 17 de noviembre de 2007), modificada por la Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público (BOE núm 164, de 10 de julio de 2015).

sector público por las empresas de contenidos al considerar que la comercialización de la información del sector público por las propias administraciones públicas puede generar problemas de competencia[12], por ejemplo, a través de la existencia de situaciones de monopolio o de subvenciones cruzadas.

De igual modo, la capacidad de almacenamiento de los equipos informáticos y la velocidad de transmisión de las actuales redes permites conexiones masivas y automatizadas. En consecuencia, los controles y limitaciones propios de las cesiones de datos personales resultan manifiestamente inadecuados[13], siendo preciso abordar un replanteamiento en cuanto a las garantías establecidas para la tutela de los distintos bienes jurídicos en juego, tanto público como privado.

Bajo la apariencia de potenciales ventajas pueden encontrarse efectos indeseables e irreversibles a evitar, sobre todo, si tenemos en cuenta que, con frecuencia, la información se pone en manos de terceros que la pueden utilizar con ánimo de lucro.

Verdaderamente, al incorporarse la información a soporte electrónico y simplificarse notablemente el acceso a través de medios telemáticos, se plantea un nuevo escenario, donde las posibilidades de su reutilización se amplían notablemente. Por tanto, la aplicación ordinaria de las nuevas

---

[12] Comisión Europea (1998) La información del sector público: un recurso clave para Europa. Libro verde sobre la información del sector público en la sociedad de la información. COM(1998) 585. Apartado 45. En algunos casos, la reutilización comercial de la información del sector público puede, no obstante, plantear dudas sobre los límites del papel que corresponde a los diferentes agentes. En cuanto los intereses del sector privado entren en el mercado de la información pública, será más difícil mantener el acceso para todos los ciudadanos. Al mismo tiempo, si el sector público añade valor a su propia información y comercializa productos de información en un mercado de la información que hasta ahora ha sido privado, puede plantearse el problema de la lealtad en la competencia. http://cordis.europa.eu/pub/econtent/docs/gp_es.pdf

[13] Véase Valero Torrijos, J.: «Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado», en Valero Torrijos, J. (coord..), *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Thomson-Aranzadi, Cizur Menor, 2013, pp. 53 a 58

tecnologías a la información administrativa es lo que facilita su posterior reutilización, por lo que está claro que nos encontramos ante un supuesto de tratamiento de información.

No obstante, tal y como se ha comentado con antelación, para que sea aplicable el derecho fundamental a la protección de datos personales es necesario que este tratamiento se sustancie sobre datos personales. Cuando la información administrativa que va a ser objeto de reutilización no contiene datos personales, no existiría ningún impedimento, al menos, desde la perspectiva del derecho fundamental a la protección de datos personales.

Así, uno de los principales desafíos consiste en replantear el cumplimiento de los límites aplicables, lo que exige en primer lugar que la información pueda ser tratada fuera de su contexto original o, al menos, de manera fragmentada, es decir, sin que sea posible reconfigurar su sentido inicial como parte de un documento formalizado o en conexión con otros datos adicionales cuando, debido a las restricciones impuestas por el régimen jurídico que regule el acceso a la misma, no se tenga reconocido el derecho a conocerla en su formato y/o soporte original debido a que la información objeto de conocimiento excedería el alcance del derecho de acceso.

El uso avanzado de medios electrónico permite desvincular los datos del documento original donde se contengan y, de este modo, llevar a cabo su procesamiento independiente[14], si bien resulta esencial que las garantías generales de los documentos en cuanto a integridad y autenticidad pueden asegurarse incluso cuando se incorporen a otros documentos o sean objeto de tratamiento.

Así pues, el documento como unidad de gestión ha de fragmentarse en atención a la información que contiene, de manera que solo se pongan a disposición de terceros aquellos datos que sean estrictamente necesarios

---

[14] En relación a las implicaciones jurídicas de este paradigma en el ámbito general de las Administraciones Públicas, véase Valero Torrijos, J.: *Derecho, innovación y Administración electrónica*, Global Las Press, Sevilla, 2013, pp. 293 a 303.

para el ejercicio de sus funciones o la satisfacción de sus derechos o intereses legítimos. Incluso, puede darse el caso de que no sea necesario a tales efectos compartir la información original, sino que, por el contrario, baste con una versión transformada de la misma que no conlleve una modificación esencial, de manera que dicha exigencia legal se vería incluso reforzada en su garantía.

Ahora bien, como señala VALERO TORRIJOS, al mismo tiempo se incrementan las dificultades desde la perspectiva de las garantías tecnológicas, ya que resulta imprescindible también asegurar la integridad y autenticidad de unidades de información de menor tamaño que aquellas que inicialmente fueron generadas por el autor del documento, cuya estructura y contenido originales no pueden desfigurarse; sin perjuicio de que, en todo caso, deban adoptarse las medidas que permitan conservar la información referida al contexto inicial del tratamiento realizado de los datos y, sobre todo, a su origen, ya que de los mismos pueden derivarse limitaciones sustanciales en cuanto a la posibilidad de reutilizar la información para otras finalidades o por otros sujetos distintos de los que recogieron los datos[15].

De este modo, el concepto de documento, entendido como un soporte en el que consta la información de manera estática y sin posibilidad alguna de tratamiento directo y automatizado, se desplaza para dejar paso al dato como elemento mínimo de gestión documental que permita su procesamiento avanzado para ofrecer nuevos servicios y funcionalidades.

Asimismo, la puesta a disposición segmentada a partir de la información relevante y no de los documentos, entendidos como conjuntos estructurados dotados de unidad que no se pueden fragmentar, permite limitar el acceso a la información a fin de lograr la protección efectiva de derechos e intereses públicos o privados que deban respetarse, tal y como sucede con la

---

[15] Véase Valero Torrijos, J. (2014). Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria. Implicaciones jurídicas desde la perspectiva de la innovación tecnológica. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Aranzadi.

intimidad la seguridad pública o, incluso, los datos de carácter personal que, aun sin ser íntimos, no esté justificada su revelación.

Partiendo de esta premisa, el desafío desde el punto de vista jurídico radica en asegurar que el tratamiento avanzado de los datos en que consiste la descontextualización no implique la pérdida de información relevante a la hora de determinar su origen y, por tanto, aplicar las limitaciones en cuanto a accesos y usos posteriores, todo ello sin permitir la identificación del titular de la información cuando dicha posibilidad se considere ilícita.

Ahora bien, los datos aislados carecen de utilidad en sí mismos considerados, por lo que resulta imprescindible vincularlos con otros obtenidos de diferentes fuentes y proveedores de información. Resulta imprescindible reforzar los incentivos para facilitar la cooperación entre los diversos sujetos que suministran los datos, de manera que su gestión agregada pueda ofrecer información valiosa para todos ellos, sin que se resientan las exigencias jurídicas en cuanto al acceso de la información y su uso para fines distintos de los que inicialmente justificaron su recogida.

En otro orden de cosas, resulta imprescindible asegurar no solo la adecuada protección de la privacidad de los sujetos afectados, sino, además y sobre todo, que dispongan de toda la información necesaria de manera transparente a la hora de la toma de decisiones que le afecten. En última instancia, cuando se pretendan ofrecer servicios en los que el usuario deba aceptar el tratamiento de su información personal, ha de garantizarse no solo que formalmente ha prestado su consentimiento sino que, además, lo ha hecho específicamente tanto por lo que respecta a la utilización de la aplicación o del producto como, además y de manera independiente, en cuanto a la cesión de sus datos personales, debiendo ser informado previamente acerca de quién llevará a cabo eventuales tratamientos de su información.

Resulta indudable que la tecnología supone una mayor interconexión potencial de los sistemas de información, de manera que se favorece la accesibilidad a los datos y asimismo se permite que se puedan actualizar o, en su caso, contrastar con los que obran en poder de otros usuarios o

entidades de procesamiento que se puede llevar a cabo de manera automatizada, es decir, sin intervención directa de personas físicas. Cuando los datos se encuentran en soporte papel, su vinculación con otros para la obtención de información de valor añadido resulta ciertamente compleja, ya que dicha operación ha de llevarse a cabo supuesto por supuesto, y de forma manual, dificultándose la opción de implantar tratamientos automatizados a menos que tenga lugar dicho procesamiento previo. Sin embargo, el uso de estándares adecuados, nos sitúa ante un escenario en el que esa labor se simplifica notablemente y, en consecuencia, se facilita el tratamiento automatizado de los datos, desplazándose el control en el acceso y posterior uso de la información de quien tiene inicialmente en su poder a quien diseña y desarrolla la correspondiente aplicación informática. Y precisamente aquí radica uno de los ejes a partir del cual tratar de superar las dificultades que, desde el punto de vista de las limitaciones jurídicas, conlleva la normativa sobre el acceso y la reutilización de la información.

Especialmente relevante resulta la exigencia de que, aun prestándose el necesario consentimiento para el procesamiento de su información personal, el uso posterior de los mismos no resulte incompatible con la finalidad que en principio justificase la recogida de los datos, supuesto en el que la obtención de un consentimiento específico y separado del primero resultaría incuestionable para garantizar que sea realmente libre.

En este sentido, el uso avanzado de medios electrónicos permite plantear que el diseño de las aplicaciones y de los sistemas de información se estructure a partir de la disociación como criterio general, de manera que a menos que resulte estrictamente imprescindible en razón de la naturaleza de los servicios los tratamientos informativos no identifiquen al usuario. Así se podría evitar la restricción que supone en algunos casos la exigencia de un consentimiento específico para usos diferentes del inicial o incluso cesiones a terceros.

Esta exigencia debería proyectarse especialmente sobre aquellos supuestos en que la información del usuario de los servicios se ponga a disposición de un tercero más allá de la relación directa que inicialmente se establezca con el prestador principal, de manera que aquél no pueda

beneficiarse del consentimiento otorgado directamente a este último para satisfacer sus propios intereses.

En definitiva, se trataría de reforzar las garantías jurídicas del titular, de manera que su información no pueda ser accesible para sujetos distintos de aquellos con los que mantiene una vinculación directa, sin perjuicio de que pueda ponerse a disposición de terceros de manera anónima o, en su caso, previa la obtención de un consentimiento específico.

A modo de conclusión, señala VALERO TORRIJOS que el artículo 18.4 de la Constitución debe extenderse más allá de las limitaciones propias de la disciplina normativa sobre la protección de los datos de carácter personal, de manera que realmente ofrezca al titular de la información la capacidad de llevar a cabo una gestión avanzada de sus datos para, en su caso y con las oportunas garantías en cuanto al anonimato, poder otorgar a posteriori su consentimiento para ciertos procesos y actuaciones distintos del inicial; y todo ello a partir de un incremento de la transparencia en cuanto a los fines, a las condiciones técnicas de los tratamientos informativos y, en general, las circunstancias en las que van a tener lugar[16].

Junto a esta perspectiva pública del principio de transparencia, se ha de manifestar la existencia de una transparencia con un sentido diferente en el ámbito privado. Una transparencia cuya finalidad reside en facilitar la demanda de información por parte de los particulares para con las empresas. Se puede comprobar que existe una preocupación cada vez mayor a la hora de obtener todo tipo de información, incluidos los procedimientos internos. Y el Ordenamiento no se queda al margen de ello, y con esta finalidad se crean instrumentos normativos para obligar a las empresas a facilitar esta información. Como derivado de este principio, se amplía el deber de responsabilidad directa o activa por parte de las mismas.

---

[16] Véase Valero Torrijos, J. (2014). Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria. Implicaciones jurídicas desde la perspectiva de la innovación tecnológica. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Aranzadi.

De este modo, el Ordenamiento jurídico relativo a la protección de datos, no permanece al margen, y la transparencia ha quedado reforzada en el RGPD como derecho no solo susceptible de articulación por los particulares ante los poderes públicos, en las relaciones verticales, sino que también se corresponde con las obligaciones positivas que pesan sobre las autoridades públicas a la hora de asegurar la protección de datos bajo el ángulo de la igualdad y equilibrio de posiciones en las relaciones entre individuos, horizontales.

Desde esta perspectiva se ha intentado abordar el presente trabajo. Se diferencia la perspectiva pública y la privada de la transparencia. Aunque en ambos sectores el derecho a la protección de datos se ve afectado, o la limita, el procedimiento de actuación y su significado es totalmente distinto. Se hace referencia a las limitaciones respecto a la solicitud de información pública por parte de la sociedad, así como la problemática que encierra la reutilización de esta información puesta en manos de la empresa privada. Todo ello, bajo el prisma del derecho a la protección de datos. De igual manera, se hace referencia a la nueva normativa de protección de datos, y las obligaciones conexas que se establecen, como elemento catalizador del consentimiento informado por parte de los interesados en relación al tratamiento de sus datos. Éste, y no otro, es el verdadero caballo de batalla en la actualidad, con unos procedimientos cada vez más técnicos y prolijos, que dificultan sobremanera la obtención real de ese consentimiento informado por parte del interesado.

CAPÍTULO Iº: LAS GARANTÍAS DEL RÉGIMEN DE LA PROTECCIÓN DE DATOS. GARANTÍAS INSTITUCIONALES Y SUBJETIVAS.

SUMARIO: 1. TRANSPARENCIA EN LA INFORMACIÓN AL INTERESADO DEL TRATAMIENTO DE SUS DATOS PERSONALES Y EN EL EJERCICIO DE SUS DERECHOS. –1.1. La novedad del principio de transparencia. –1.2. El deber de suministrar información al interesado (artículos 13 y 14). –1.3. El Derecho de acceso del interesado (art. 15). –1.4. Conclusiones. –2. EL DERECHO DE RECTIFICACIÓN, CANCELACIÓN, LIMITACIÓN DEL TRATAMIENTO, OPOSICIÓN Y DECISIONES INDIVIDUALES AUTOMATIZADAS. –2.1. Introducción y consideraciones previas. –2.2. El derecho a la rectificación. –2.3. El derecho a la cancelación. –2.4. La limitación del tratamiento. –2.5. Derecho de oposición. –2.6. Decisiones individuales automatizadas. –3. LOS PRINCIPIOS DE PROTECCIÓN DE DATOS DESDE EL DISEÑO Y PROTECCIÓN DE DATOS POR DEFECTO. –3.1. Concepto y contenido de ambos principios. –3.2. Su regulación en el RGPD. –3.3. Medidas concretas para la observancia de estos principios por los responsables del tratamiento y por los productores de servicios, aplicaciones y productos. –3.4. Transparencia y Protección de datos desde el diseño. –3.5. Conclusión. –4. EL DERECHO A LA PORTABILIDAD DE LOS DATOS. –4.1. Antecedentes. –4.2. Requisitos del Derecho a la Portabilidad en el RGPD. –4.3. Contenido del derecho a la portabilidad. –4.4. Portabilidad en el marco del derecho de la competencia. –5. LA NOTIFICACIÓN DE LAS VIOLACIONES DE SEGURIDAD. –5.1. Introducción y conceptos sobre seguridad de los datos y violaciones de seguridad. –5.2. Marco normativo relacionado con las violaciones de seguridad. –5.3. El daño reputaciones en las organizaciones obligadas a la notificación por ser víctimas de una violación de seguridad.

1 LAS GARANTÍAS DEL RÉGIMEN DE PROTECCIÓN DE DATOS.

El régimen de Protección Datos, en el ordenamiento jurídico español tiene un preciso anclaje constitucional en el artículo 18.4 CE que establece, dentro del ámbito de la protección de la intimidad de la persona, una garantía legal específica de la misma intimidad y del ejercicio de los derechos y deberes constitucionales, en relación con el uso automatizado de la información personal.

Esta misma previsión ha dado que a la configuración doctrinal y constitucional de un verdadero derecho fundamental a la protección de datos, que en consonancia con el enfoque internacional sobre el este problema, le ha dado un potente sentido subjetivo a este problema, muy relacionado con un poder de disposición de los individuos sobre la utilización

de su información personal. La máxima expresión de construcción de base subjetiva son el principio de consentimiento –que se analiza en el capítulo siguiente- y los derechos denominados ARCO[17] normalmente considerados como un elemento que refuerza el control de los interesados sobre el tratamiento de sus datos.

Tales derechos, ya recogidos en los primeros textos internacionales de la materia que inspiraron nuestra primera legislación de protección de datos, y recogidos en nuestra legislación vigente, aparecen, como no podía ser de otra forma en el RGPD y la Directiva 95/46/CE.

2 LOS DERECHOS DE RECTIFICACIÓN, CANCELACIÓN, LIMITACIÓN DEL TRATAMIENTO, OPOSICIÓN Y DECISIONES INDIVIDUALES AUTOMATIZADAS

2.1 Introducción y consideraciones previas

Uno de los elementos característicos del RGPD es el refuerzo de la posición de control del individuo con respecto a sus propios datos personales, lo que se traduce en un mayor elenco de derechos de los interesados. Este refuerzo se traducirá en un fortalecimiento de las obligaciones del responsable del tratamiento.

Los derechos de rectificación, cancelación, oposición y limitación del tratamiento están estrechamente relacionados con el concepto de autodeterminación informativa y el control por parte del individuo sobre sus propios datos. A este respecto, MURILLO DE LA CUEVA define la autodeterminación informativa como «el control que a cada uno de nosotros nos corresponde sobre la información que nos concierne personalmente, sea íntima o no, para preservar de este modo y en último extremo la propia

[17] Acrónimo que hace referencia al derecho de acceso, al de rectificación, al de cancelación y al de oposición, ARCO.

identidad, nuestra dignidad y libertad. En su formulación como derecho, implica necesariamente poderes que permitan a su titular definir los aspectos de su vida que no sean públicos, que desea que no se conozcan, así como facultades que le aseguren que los datos que de su persona manejan terceros informáticamente son exactos, completos y actuales, y que se han obtenido de modo leal y lícito»[18].

En ese sentido, la autodeterminación informativa, estrechamente relacionada con los tradicionales derechos ARCO, se concreta en las siguientes facultades:

> *«1) ser informado en la recogida de datos, 2) conocer la existencia de ficheros y tratamientos de datos personales, 3) acceder a ellos para comprobar qué información personal del afectado contienen, 4) obtener la rectificación de los que no sean exactos, 5) obtener la cancelación de los que no deban ser tratados o hayan perdido la calidad que en su día justificó el tratamiento, 6) oponerse a un tratamiento cuando no sea necesario conforme a la ley el consentimiento del afectado y concurran motivos fundados y legítimos relativos a su concreta situación personal, 7) no sufrir perjuicios como consecuencia de decisiones tomadas exclusivamente en virtud de perfiles personales obtenidos informáticamente, 8) ser resarcido de los perjuicios sufridos a causa de tratamientos que no se ajusten a las condiciones legalmente establecidas, 9) ser protegido por las instituciones especializadas creadas* ex profeso *para defender este derecho fundamental»[19].*

En esencia, las facultades de control del interesado con base en la denominada autodeterminación informática no han variado. Sin embargo, el

---

[18] Murillo de la Cueva, P. L. (1993). Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal). Madrid: Centro de Estudios Constitucionales, pp. 32 y ss.

[19] Murillo de la Cueva, P. L. (2007). Perspectivas del derecho a la autodeterminación informativa. *IDP. Revista de Internet, Derecho y Política, 5, p. 20*. DOI: http://doi.org/10.7238/idp.v0i5.438

avance de las nuevas tecnologías y la digitalización de la sociedad y de las empresas ha requerido la revisión y adaptación de la normativa a la nueva era digital, incluyendo la modificación de los concretos derechos del interesado, con la adición de nuevos derechos. En cierto sentido, ya no podemos hablar de los derechos ARCO[20].

Así, el hecho de que la cancelación, supresión, rectificación o las propias decisiones individuales automatizadas, tengan que estar sometidas a una serie de garantías, está en estrecha relación con el derecho al libre desarrollo de la personalidad, elemento clave en la protección de datos de carácter personal. En relación con el ejercicio de los derechos de los interesados y los plazos, el responsable dispone de un mes para facilitar la información a los interesados sobre el curso de sus solicitudes en relación con el ejercicio de sus derechos, artículos 15 a 22 del RGPD, prorrogable por otros dos meses[21].

El Reglamento incorpora novedades sustanciales para adaptar los clásicos derechos ARCO a la era digital, dominada por avances tecnológicos, algoritmos y el mundo online. Se puede afirmar que con el nuevo RGPD, se pretende mejorar sustancialmente la capacidad de decisión y control de los ciudadanos sobre los datos que confían a terceros. A modo de ejemplo, y

---

[20] Jornada de ENATIC sobre el Reglamento General de Protección de Datos 29 de abril de 2016. Consejo General de la Abogacía Española en Paseo de Recoletos núm 13. Madrid. Según el profesor Piñar, con esta nueva norma se acabaron los conocidos en España como derecho ARCO (Acceso, Rectificación, Cancelación y Oposición). El nuevo RGPD se refiere ahora a los derechos de Transparencia (art. 12), Información (arts. 13 a 14), Acceso (art. 15), Rectificación (Art. 16), Supresión o derecho al olvido (art. 17), Limitación del tratamiento (art. 18), Portabilidad de datos (art. 20) y Oposición (art. 21).

[21] El Considerando 59 del RGPD señala que «deben arbitrarse fórmulas para facilitar al interesado el ejercicio de sus derechos en virtud del presente Reglamento, incluidos los mecanismos para solicitar y, en su caso, obtener de forma gratuita, en particular, el acceso a los datos personales y su rectificación o supresión, así como el ejercicio del derecho de oposición. El responsable del tratamiento también debe proporcionar medios para que las solicitudes se presenten por medios electrónicos, en particular cuando los datos personales se tratan por medios electrónicos. El responsable del tratamiento debe estar obligado a responder a las solicitudes del interesado sin dilación indebida y a más tardar en el plazo de un mes, y a explicar sus motivos en caso de que no fuera a atenderlas».

sin pretender ser exhaustivos, se puede señalar que la transparencia llegará incluso a abarcar aspectos como la explicación sobre la lógica de los algoritmos, en relación con las decisiones automatizadas que produzcan efectos jurídicos para los interesados. Los derechos de los interesados se ven reforzados en lo que respecta a las decisiones individuales automatizadas, para el caso de que éstas tengan efectos jurídicos para el interesado, desde el momento en que éste tendrá derecho a recibir una explicación sobre la lógica del algoritmo, a expresar su punto de vista, a pedir la intervención humana e impugnar la decisión. En el derecho de rectificación queda de manifiesto la posibilidad de una declaración adicional para completar el dato inexacto, incompleto o erróneo. En lo que respecta al derecho de oposición, se incluye expresamente dicho derecho en el ámbito de la elaboración de perfiles, así como cuando el tratamiento tenga por fin la mercadotecnia directa. Asimismo, se contempla la limitación del tratamiento para una serie de supuestos tasados referentes a ilicitud, inexactitud, reclamaciones y cuando el interesado lo solicite como medida provisional en caso de no haber ejercido el derecho de oposición.

2.2 El derecho a la rectificación

Ya desde los Considerandos del RGPD se reconoce que «deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos»[22] y que «los interesados deben tener derecho a que se rectifiquen los datos personales que le conciernen […]»[23].

Por su parte, el apartado d) del artículo 5.1 RGPD relacionado con los principios del tratamiento reconoce que «los datos personales serán exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos

[22] Véase al respecto el Considerando 39 RGPD.

[23] Así se reconoce expresamente en el Considerando 65 del RGPD.

personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»)». Y en el artículo 16 RGPD se destaca que:

> *«El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional».*

Tradicionalmente, el derecho a la rectificación se ha caracterizado por permitir corregir errores, modificar los datos que resulten ser inexactos y garantizar la certeza de la información objeto de tratamiento. El derecho de rectificación, junto con el derecho de cancelación, forma parte del contenido esencial del derecho a la protección de datos[24].

---

[24] Véase al respecto Abad Amorón, M. R. (1993). Libertad informática y nuevos derechos: una polémica legislación. *Revista Telos*, *33*. «La posibilidad de que se rectifiquen los datos ha de formar parte necesaria del contenido de las leyes de protección de datos; asimismo supone una consecuencia lógica del ejercicio del derecho de acceso pudiendo afirmarse, que es una de sus finalidades». El artículo se encuentra accesible en el siguiente link: https://telos.fundaciontelefonica.com/telos/anteriores/num_033/inves_legislacion0.html En sentido contrario, véase la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación, BOE núm. 25 de 29 de enero de 1998, en donde el apartado 2 de su norma primera expresamente declara que «la Ley configura los derechos de acceso, rectificación y cancelación como derechos independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro». El texto completo de la Instrucción se encuentra disponible en el siguiente link https://www.boe.es/boe/dias/1998/01/29/pdfs/A03058-03060.pdf Son numerosos los autores que han destacado la interrelación y conexión del derecho de acceso con los derechos de rectificación y cancelación. Véase, entre otros, Serrano Pérez, M.M.: «El derecho fundamental a la protección de datos. Su contenido esencial», *Nuevas políticas públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, núm. 1, 2005, pp. 258 y ss. «no están absolutamente desconectados entre sí, ni desde una perspectiva legal ni desde una perspectiva instrumental. Esta última, a nuestro juicio, se sigue manifestando en la configuración del derecho de acceso como paso previo para proceder posteriormente a la rectificación o a la cancelación, según el resultado de la información conocida tras el acceso, lo cual tampoco significa que la rectificación y la cancelación no puedan tener su origen en el conocimiento de los datos siguiendo un camino distinto del ejercicio del derecho de acceso. Por ello podemos señalar que la dependencia no implica el ejercicio previo de ninguno de ellos, en el sentido de no convertirse en requisito exigido por el responsable del tratamiento, y que justifique desde esa óptica su denegación».

2.3 El derecho a la cancelación

Con el RGPD se produce un cambio de denominación y, donde se venía haciendo tradicionalmente referencia a la cancelación de datos de carácter personal, pasa a utilizarse la expresión «derecho a la supresión», y se recoge en el artículo 17 del RGPD, en un contexto más amplio que el tradicional derecho a la cancelación:

> *«1.El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concurra alguna de las circunstancias siguientes: […] ».*

Conforme al artículo 4.2 del RGPD, la supresión en sí misma implica un tratamiento[25] de datos de carácter personal. Con el fin de garantizar un tratamiento leal y transparente, el responsable del tratamiento debe facilitar al interesado información sobre el derecho a solicitar la supresión.

2.4 La Limitación del tratamiento

El artículo 18 del Reglamento contempla un derecho del interesado a obtener del responsable del tratamiento la limitación de datos tratamiento cuando se cumpla alguna de las siguientes condiciones: «i) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; ii) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; iii) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; iv)

---

[25] El RGPD define el tratamiento como «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, *supresión* o destrucción».

el interesado se haya opuesto al tratamiento en virtud del artículo 21.1[26], mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado».

La limitación del tratamiento está contemplada para una serie de supuestos tasados, que hacen referencia a la inexactitud, ilicitud, reclamaciones y cuando el interesado lo solicite como medida provisional en caso de no haber ejercido el derecho de supresión o en caso de haber ejercido el derecho de oposición mientras se verifica si prevalecen los legítimos motivos del responsable del tratamiento sobre los del interesado.

La definición de lo que debemos de entender por limitación del tratamiento se recoge en el propio articulado del RGPD. Así, el apartado 3 del artículo 4 recoge expresamente que será «el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro».

Cuando se haya limitado el tratamiento, los datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante de la Unión o de un determinado Estado miembro. De igual modo, existe un deber de información por parte del responsable del tratamiento a todo interesado que haya obtenido la limitación del tratamiento. Esta información se deberá llevar a cabo antes del levantamiento de dicha información[27].

Por otro lado, el Considerando 67 del RGPD nos ofrece una lista no taxativa, ni cerrada de los métodos que se pueden utilizar para limitar el tratamiento de datos personales De este modo, expresamente se estipula que «entre los métodos para limitar el tratamiento de datos personales cabría incluir los consistentes en trasladar temporalmente los datos seleccionados a otro sistema de tratamiento, en impedir el acceso de usuarios a los datos

[26] El RGPD regula en el artículo 21 el denominado derecho de oposición. Se hará referencia al mismo en el siguiente apartado.

[27] Véanse los párrafos 2 y 3 del artículo 18 RGPD.

personales seleccionados o en retirar temporalmente los datos publicados de un sitio internet. En los ficheros automatizados la limitación del tratamiento debe realizarse, en principio, por medios técnicos, de forma que los datos personales no sean objeto de operaciones de tratamiento ulterior ni puedan modificarse. El hecho de que el tratamiento de los datos personales esté limitado debe indicarse claramente en el sistema».

2.5 Derecho de oposición

El interesado puede ejercer en todo momento el derecho de oposición para oponerse al tratamiento de sus catos de carácter personal, incluyendo la elaboración de perfiles, así como cuando el tratamiento tenga por objeto la mercadotecnia directa. Así se reconoce en el artículo 21[28] del RGPD.

No obstante, no nos encontramos ante un derecho absoluto. El propio artículo ofrece la posibilidad de que el responsable del tratamiento continúe tratando los datos cuando acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las

[28] El RGPD expresamente reconoce el derecho de oposición en los siguientes términos: «1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones. 2.Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia. 3.Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines. 4.A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información. 5.En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas. 6.Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público».

libertades del interesado, o para la formulación, ejercicio o defensa de reclamaciones. Asimismo, y en relación con datos personales que se traten con fines de investigación científica o histórica o fines estadísticos, el interesado tendrá el derecho de oposición, salvo que fuese necesario el tratamiento para el cumplimiento de una misión realizada por razones de interés público.

El interesado debe tener derecho a oponerse al tratamiento de cualquier dato personal relativo a su situación particular, aun en los supuestos en los que los datos personales puedan ser tratados lícitamente, porque el tratamiento sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento o por motivos de intereses legítimos del responsable o de un tercero[29].

Por su parte, y en relación con la elaboración de perfiles, el Considerando 70 del RGPD destaca que «si los datos personales son tratados con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse a dicho tratamiento, inclusive a la elaboración de perfiles en la medida en que esté relacionada con dicha mercadotecnia directa, ya sea con respecto a un tratamiento inicial o ulterior, y ello en cualquier momento y sin coste alguno. Dicho derecho debe comunicarse explícitamente al interesado y presentarse claramente y al margen de cualquier otra información».

2.6 Decisiones individuales automatizadas

Todo interesado tiene el derecho a conocer y a que se le comunique, la lógica implícita en todo tratamiento automático de datos personales y, por lo

[29] Interesa destacar que será el responsable el que demuestre que sus intereses legítimos imperiosos prevalecen sobre los intereses o los derechos y libertades fundamentales del interesado. Véase el Considerando 69 in fine del RGPD.

menos, cuando se base en la elaboración de perfiles[30], las consecuencias que se derivan de dicho tratamiento[31].

Por su parte, en el Considerando 71 del texto se recoge que «el interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar […]».

Se establece que este tipo de tratamiento incluye la elaboración de perfiles consistente en cualquier forma de tratamiento de los datos personales que evalúe aspectos personales relativos a una persona física, en particular para analizar o predecir aspectos relacionados con el rendimiento en el trabajo, la situación económica, la salud, las preferencias o intereses personales, la fiabilidad o el comportamiento, la situación o los movimientos del interesado, en la medida en que produzca efectos jurídicos en él o le afecte significativamente de modo similar. Con todo, no nos hallamos ante una prohibición absoluta, sino que, en ocasiones, y bajo determinadas circunstancias, se deben permitir las decisiones basadas en tal tratamiento, incluida la elaboración de perfiles. En este sentido, el propio Considerando 71 continúa señalando que deben permitirse bajo la condición de que lo autorice « expresamente el Derecho de la Unión o de los Estados miembros aplicable al responsable del tratamiento, incluso con fines de control y prevención del fraude y la evasión fiscal, realizada de conformidad con las reglamentaciones, normas y recomendaciones de las instituciones de la

---

[30] La expresión «elaboración de perfiles» aparece recogida en el apartado 4 del artículo 4 del RGPD. De esta forma, debemos entender por tal «toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física».

[31] Así se reconoce expresamente en el Considerando 63 del RGPD, «todo interesado debe, por tanto, tener el derecho a conocer y a que se le comuniquen, en particular, los fines para los que se tratan los datos personales, su plazo de tratamiento, sus destinatarios, la lógica implícita en todo tratamiento automático de datos personales y, por lo menos cuando se base en la elaboración de perfiles, las consecuencias de dicho tratamiento».

Unión o de los órganos de supervisión nacionales y para garantizar la seguridad y la fiabilidad de un servicio prestado por el responsable del tratamiento, o necesario para la conclusión o ejecución de un contrato entre el interesado y un responsable del tratamiento, o en los casos en los que el interesado haya dado su consentimiento explícito. En cualquier caso, dicho tratamiento debe estar sujeto a las garantías apropiadas, entre las que se deben incluir la información específica al interesado y el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión».

A mayor abundamiento, el artículo 22 del RGPD ratifica que podrán tomarse decisiones automatizadas, incluyendo la elaboración de perfiles, en los supuestos en que: i) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado; ii) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento, o iii) se basa en el consentimiento explícito del interesado.

No obstante, en estos dos últimos casos, son necesarias una serie de garantías y salvaguardas, como el derecho a obtener intervención humana por parte del responsable, derecho a que el interesado exprese su punto de vista, y derecho a impugnar la decisión adoptada.

Por último, destacamos dos restricciones a la hora de tomar las decisiones basadas únicamente en el tratamiento automatizado. Por un lado, las decisiones «no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del

interesado».[32] Por otro, tales medidas no pueden afectar a un menor. Así se recoge en el primer párrafo in fine del Considerando 71 del RGPD.

3 LOS PRINCIPIOS DE PROTECCIÓN DE DATOS DESDE EL DISEÑO Y PROTECCIÓN DE DATOS POR DEFECTO

El nuevo RGPD establece los principios de protección de datos desde el diseño y por defecto, que responden a la idea de que las leyes y la política ya no son suficientes para proteger a la intimidad[33]. Así, la propia Agencia Española de Protección de Datos ha señalado en relación a las medidas que introduce el RGPD[34]:

> *«El Reglamento supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos. Pero ello no implica necesariamente ni en todos los casos una mayor carga. En muchos casos será sólo una forma de gestionar la protección de datos distinta de la que se viene empleando ahora. En primer lugar, algunas de las medidas que introduce el Reglamento son una continuación o reemplazan a otras ya existentes, como es el caso de las medidas de seguridad o de la obligación de documentación y, hasta cierto punto, la evaluación de impacto y la consulta a Autoridades de supervisión. Otras constituyen la formalización en una norma legal de prácticas ya muy extendidas en las empresas o que, en todo caso, formarían parte de una correcta*

[32] Véase al respecto el artículo 22.4 RGPD.

[33] Véase al respecto la Resolución sobre Privacidad desde el Diseño (2010). XXXII Conferencia Internacional de Autoridades de Protección de Datos, de 27-29 de octubre de 2010. En https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

[34] Agencia Española de Protección de Datos (2016). El Reglamento de Protección de Datos en 12 preguntas. Recuperado de: http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2016/notas_prensa/news/2016_05_26-ides-idphp.php

puesta en marcha de un tratamiento de datos, como pueden ser la privacidad desde el diseño y por defecto, la evaluación de impacto sobre protección de datos en ciertos casos o la existencia de un delegado de protección de datos […]»

Afirma DUASO CALÉS[35] que la formulación de estos principios en el texto europeo se corresponde con la idea que subyace de la metodología basada en el análisis de riesgos[36]. Este análisis nos llevará a constatar que dichos principios representan medidas que se inscriben en el nuevo régimen de responsabilidad que ha diseñado el texto europeo. Los principios de la protección de datos desde el diseño y por defecto se aplicarán en función de lo que resulte de este análisis de riesgos, así como de la evaluación de aspectos referidos al tratamiento de datos personales. De este modo, todo tratamiento de datos personales, ya sea por el sector público o por el privado, implica que haya que considerar el riesgo, siendo la «aproximación basada en el riesgo» el criterio fundamental[37] en torno al que gira el RGPD.

---

[35] Duaso Calés, R. (2016). Los principios de protección de datos desde el diseño y protección de datos por defecto. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus, p 297.

[36] Con carácter general, el riesgo es la contingencia o proximidad de un daño. Aplicado a la protección de datos, se trata de la posibilidad de que se produzca un daño para la persona derivado del tratamiento de sus datos personales. Tradicionalmente, los riesgos se han tratado de forma no estructurada, mediante soluciones puntuales tomadas como acción correctiva a un accidente o incidente ocurrido y con el daño ya causado. La Gestión del riesgo es un conjunto de técnicas y herramientas de apoyo y ayuda para tomar las decisiones apropiadas, de una forma lógica, teniendo en cuenta la incertidumbre, la posibilidad de futuros sucesos y los efectos sobre los objetivos acordados; y tiene como objeto la prevención de los mismos en lugar de la corrección y la mitigación de daños una vez que éstos se han producido, por lo que resulta claramente ventajoso para las organizaciones que adopten y pongan en uso herramientas y mecanismos de Gestión de riesgos. La Norma ISO 9001:2015 está orientada hacia un enfoque preventivo que se acentúa con los aspectos referidos a la Gestión del Riesgo, que consisten en reconocer los riesgos dentro de una organización y llevar a cabo las actuaciones necesarias para evitar que se produzcan. La nueva Norma ISO 9001:2015 y la norma ISO 31000 para "Gestión de Riesgos" establecen una serie de principios que deben ser satisfechos para hacer una gestión eficaz del riesgo, de forma que se desarrollen, implementen y si es aplicable, se integren con el resto de los sistemas de gestión disponibles en la empresa.

[37] Maldoff indica que el RGPD «adopta una aproximación basada en el riesgo a la protección de datos» Maldoff, G. (2016) The Risk-Based Approach in the GDPR: Interpretation and Implications. *IAPP*. En https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf

3.1 Concepto y contenido de ambos principios

Los conceptos de *Privacy by Design* y de *Privacy by Default* encarnan un modelo de protección de la privacidad que en el futuro deberá estar basado en un modelo de operar por defecto de toda organización[38]. Los principios de la protección de datos desde el diseño y de la protección de datos por defecto, que nacieron de aquellos conceptos, responden a la necesidad de que la propia tecnología juegue un papel central en la protección de la privacidad, tanto en el desarrollo, como en el funcionamiento de toda innovación de carácter tecnológico que comporte el tratamiento de datos personales.

El concepto del *Privacy by Design* ha sido desarrollado por el Information and Privacy Commissioner of Ontario[39] de Canadá desde los años 90, y aparece por primera vez[40] en un informe que realiza esta autoridad de control con la autoridad de control holandesa, publicado en 1995[41].

Con anterioridad, se ha indicado que durante el año 2010 se adoptó en Jerusalén una Resolución[42] a nivel mundial sobre el principio de *Privacy by Design*, ésta se aprobó en la Conferencia Anual sobre protección de datos y Autoridades de protección de datos. Se recogió la idea de que la privacidad esté integrada directamente en todo sistema tecnológico, así como en todo

---

[38] «Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with legislation and regulatory frameworks; rather, privacy assurance must become an organization's default mode of operation». Cavoukian A. (2009). *Privacy by Design*., p. 1. Recuperado de: https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf.

[39] La página web del Comisionado se puede consultar en: https://www.ipc.on.ca/

[40] Hustinx, P. «Privacy by Design: Delivering the promises», *Identity in the Information Society* 3(2):253-255, agosto 2010. Este autor identifica el primer Informe en el que aparece el concepto de *Privacy by Design*

[41] Information and Privacy Commissioner, Ontario, Canada and Registratiekamer, the Netherlands, *Privacy-enhancing technologies: the path to anonymity, Volume 1*. Technical report, 1995

[42] 32nd International Conference of Data Protection and Privacy Commissioners Jerusalem, Israel. 27-29 octubre, 2010. Resolution on Privacy by Design. El texto completo se puede consultar en https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

proceso que comporte el tratamiento de datos personales Viene a reconocer la privacidad por diseño como un componente esencial de la protección de la privacidad. Aquel principio responde a una filosofía y a un enfoque por el que se implanta la privacidad en el propio diseño, así como en la gestión de las tecnologías y sistemas de información durante todo el ciclo de la información.

Por su parte, la Federal Trade Commission inserta el principio al que nos referimos como uno de los pilares de su Privacy Framework[43] que tiene por objetivo articular las mejores prácticas para las empresas que tratan datos de consumidores. Las tres prácticas a adoptar son:

> *«i) Privacy by Design; ii) Simplified Choice for Businesses; y iii) Greater Transparency. En relación al principio Privacy by Design, el Informe recoge expresamente como principio básico, que las compañías deberían promocionar la privacidad de los consumidores en todas sus divisiones y en cada etapa del desarrollo de sus productos y servicios»[44].*

Atendiendo al Principio final que propone el Informe, las empresas deben incorporar protecciones sustantivas de privacidad en sus prácticas, tales como: i) seguridad de los datos. Las empresas deben proporcionar una seguridad razonable respecto a los datos de los consumidores; ii) limitación razonable de su acumulación. Las empresas deben limitar su recopilación de datos; iii) prudente retención de datos. Las empresas deben implementar políticas razonables de retención y eliminación de los datos; y iv) exactitud.

---

[43] Federal Trade Commission, Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. Texto completo del Informe disponible: https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

[44] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*. p. 22 « Baseline Principle: Companies should promote consumer privacy throughout their organizations and at every stage of the development of their products and services».

Las empresas deben mantener una exactitud razonable de los datos de los consumidores[45].

De igual modo, en el ámbito europeo, la Asociación Europea de Consumidores (BEUC), también se encuentra interesada por el principio de Privacy by Design. En su contestación a las propuestas de reforma de la protección de datos, insta[46] a la Comisión Europea a incluir la privacidad desde el diseño como un principio explícito y obligatorio en el nuevo Marco para la Protección de Datos.

Por otro lado, el Supervisor Europeo de Protección de Datos expresaba su voluntad[47] de que este principio formara parte de la nueva legislación en la materia:

> *«Privacy by design refers to the integration of data protection and privacy from the very inception of new products, services and procedures that entail the processing of personal data. According to*

---

[45] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers*. p. 30 « Final Principle: Companies should incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention and disposal practices, and data accuracy».

[46] «A comprehensive approach on personal data protection in the European Union» European Commission's Communication BEUC, The European Consumers' Organisation's response, 24 de enero de 2011, p. 13 «BEUC urges the European Commission to include privacy by design as an explicit, mandatory principle in the new Framework for Data Protection. Privacy and security by design should require privacy and security to be embedded in ICT technologies during the whole life cycle, from the design of specifications of systems and technologies. This would make its implementation compulsory by both ICT manufacturers and data controllers, while providing for its effective enforcement by Data Protection Authorities. BEUC firmly believes that this principle should be technology neutral to apply across the sectors, from transport and health systems to social networks and ICT devices. The principle could be further specified in sector-specific legislation. Such technical solutions should comply with the principles of data minimisation, transparency, data confidentiality, purpose limitation, data security and foster consumer empowerment». Texto accesible en el link http://ec.europa.eu/justice/news/consulting_public/0006/contributions/organisations/beuc_en.pdf

[47] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", 14 de enero de 2011, p. 23 https://secure.edps.europa.eu/EDPSWEB/webdav/shared/Documents/Consultation/Opinions/2011/11-01-14_Personal_Data_Protection_EN.pdf.

the EDPS privacy by design is an element of accountability. Accordingly, data controllers would also be required to demonstrate that they had implemented privacy by design, where appropriate».

El Grupo de trabajo de protección de datos del artículo 29 señalaba[48] igualmente en el año 2012 que la inclusión en el Reglamento de los principios de protección de datos desde el diseño y por defecto es uno de los aspectos positivos del mismo:

«Para los responsables del tratamiento de datos, el Reglamento simplifica y aporta una mayor coherencia, un mayor hincapié en su responsabilidad por los datos que traten y la necesidad de demostrar esto con una protección desde el diseño*, una protección por defecto, evaluaciones de impacto sobre la intimidad, nombramiento de un responsable de protección de datos, obligación de notificación de violación de datos y adopción de un enfoque cautelar en las transferencias internacionales. Además, las normas corporativas vinculantes se reconocen expresamente como instrumento para enmarcar las transferencias internacionales de datos».*

En el contexto actual, dominado por unas tecnologías que permiten una interconexión permanente y una circulación sin límites de la información de carácter personal, integrar la privacidad en la arquitectura de todo sistema o aplicación, así como en el diseño de aquellos procesos que conllevan el tratamiento de datos constituye una respuesta que puede traer resultados que ayuden al cumplimiento de los principios de protección de datos que las leyes establecen.

El concepto de Privacy by Design está basado en un enfoque proactivo y no tanto en la reacción ante la vulneración del derecho a la privacidad[49]. Se

---

[48] Grupo de Trabajo de Protección de Datos del Artículo 29, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_es.pdf.

[49] Véase Cavoukian, A.: *Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices*, 25 de mayo de 2010, p. 2. Texto completo disponible en http://www.ontla.on.ca/library/repository/mon/24005/301946.pdf

basa fundamentalmente en una visión de prevención. Al aplicar este principio, se van a poder limitar los riesgos en lo relativo a los tratamientos de datos. Podríamos identificar en la adopción del concepto de Privacy by Design, una referencia al principio de precaución. Éste ha sido contemplado como un factor de ralentización de la innovación tecnológica. Sin embargo, para la doctrina[50] aparece como una condición para crear la confianza de los ciudadanos en el desarrollo de las tecnologías de la información y las comunicaciones. La aplicación del principio de precaución se justificaría fácilmente atendiendo a la importancia de los riesgos a los que se pueden enfrentar nuestras sociedades como consecuencia de ciertas tecnologías.

Precisamente por tener su aplicación en el momento de la creación de la propia tecnología, teniendo como objetivo que la privacidad esté integrada en el sistema o solución tecnológica para reducir al máximo la posibilidad de que los riesgos que en materia de protección de datos puedan materializarse, el concepto de Privacy by Design puede verse como una manifestación de la aplicación del principio de precaución.

Con el fin de que los objetivos del concepto de Privacy by Design se vean alcanzados, es importante que se cumplan los que se han denominado[51] los «Siete principios fundamentales»[52] de este concepto[53]:

---

[50] Yves Poullet, «Internet et Sciences Humaines ou «Comment comprendre l'invisible?», *Revue des Questions Scientifiques*, 2011, 182 (4) : 377-398, p. 390. https://www.unamur.be/sciences/philosoc/revueqs/textes-en-ligne/RQS_182_4Internet.pdf

[51] Véase al respecto Cavoukian, A. (2010). Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices, p. 2 Una versión resumida del texto anteriormente comentado, puede consultarse en el siguiente link https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[52] Una versión en español del texto completo se encuentra disponible en el siguiente link https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf

[53] Por su indudable interés junto con los Siete principios fundamentales, incluiré unas notas explicativas o aclaratorias de los mismos que han sido publicadas por García Herrero, J. en formato de dos entradas de su blog. Véase al respecto las siete próximas notas a pie de página, una por cada principio. El contenido completo de las entradas se encuentra accesible en http://jorgegarciaherrero.com/privacidad-desde-el-diseno-o-privacy-by-design-i/ y

«1. Proactivo, no Reactivo; Preventivo no Correctivo. El enfoque de Privacidad desde el Diseño (PbD por sus siglas en inglés) está caracterizado por medidas proactivas, en vez de reactivas. Anticipa y previene eventos de invasión de privacidad antes de que estos ocurran. PbD no espera a que los riesgos se materialicen, ni ofrece remedios para resolver infracciones de privacidad una vez que ya ocurrieron – su finalidad es prevenir que ocurran. En resumen, Privacidad por Diseño llega antes del suceso, no después[54].

2. Privacidad como la Configuración Predeterminada. Todos podemos estar seguros de una cosa – ¡Lo predeterminado es lo que manda! La Privacidad por Diseño busca entregar el máximo grado de privacidad asegurándose de que los datos personales estén protegidos automáticamente en cualquier sistema de IT dado o en cualquier práctica de negocios. Si una persona no toma una acción, aun así la privacidad

---

http://jorgegarciaherrero.com/privacidad-desde-el-diseno-en-el-reglamento-general-de-proteccion-de-datos-y-ii/

[54] Protección Preventiva. Proactividad. El concepto "Privacy by Design" adelanta la barrera de protección de la privacidad, se anticipa a la causación de posibles daños. Cualquier tecnología informática, actividad empresarial o infraestructura en red destinada a lidiar con datos personales debe ser concebida y diseñada desde cero identificando a priori los posibles riesgos que pueda suponer para la privacidad de esos datos, y minimizando esos riesgos antes de que puedan concretarse en daños, antes incluso de que el sistema o tecnología llegue a entrar en funcionamiento. No se trata de reaccionar, subsanar o paliar los daños que hayan llegado a producirse (como hasta ahora), sino de prevenirlos, identificando las debilidades de los sistemas o aplicaciones para neutralizarlos o minimizar su riesgo antes de que esos riesgos se concreten en daños. No hay, desde luego, una sola manera, o un procedimiento estándar para conseguir este objetivo. El mapa de riesgos, y la tecnología más adecuada para prevenirlos dependerá en cada caso del objetivo o funcionalidad perseguido, y del contexto. A tal efecto: i) La implementación de la Privacidad desde el diseño debe ser impuesta desde el escalón de poder más alto de la empresa u organización; ii) Es preciso asegurarse de que esta implementación se concreta en acciones, y no queda sólo en políticas o en "papel mojado"; iii)Es imprescindible asignar la responsabilidad sobre ese diseño, aplicación y cumplimiento a una o varias personas determinadas; iv) También es importante la formación al personal en la importancia de la nueva política y las obligaciones derivadas de la misma; v) Se implementarán procedimientos para la detección temprana de diseños, prácticas y resultados deficientes en materia de privacidad, y se auditará la efectividad de su funcionamiento. Se desarrollará preventivamente un procedimiento para gestionar contingencias "data breach". Este compromiso con la protección de la privacidad debe ser compartido con la comunidad de usuarios y promovido en el resto de empresas o instituciones que interactúen con la nuestra.

se mantiene intacta. No se requiere acción alguna de parte de la persona para proteger la privacidad – está interconstruida en el sistema, como una configuración predeterminada[55].

3. Privacidad Incrustada en el Diseño. La Privacidad por Diseño está incrustada en el diseño y la arquitectura de los sistemas de Tecnologías de Información y en las prácticas de negocios. No está colgada como un suplemento, después del suceso. El resultado es que la privacidad se convierte en un componente esencial de la funcionalidad central que está siendo entregada. La privacidad es parte integral del sistema, sin disminuir su funcionalidad[56].

---

[55] Los datos personales estarán protegidos por defecto en cualquier sistema. Más aún: la configuración por defecto será la más segura posible en términos de privacidad. La privacidad del usuario debe estar automáticamente protegida al máximo nivel sin necesidad de que éste tenga que hacer nada. Esta idea no se limita a las opciones que el usuario puede configurar, sino a todas las opciones del sistema como un todo. La principal manifestación de este principio es la exigencia de "minimización de datos". No se deben recoger, almacenar ni tratar datos personales, salvo que sea imprescindible para la finalidad perseguida. Los datos que sí sean recogidos, serán objeto de medidas técnicas y organizativas de seguridad. Las más eficaces en cada caso, encriptación, seudonimización, separación de datos, de funciones y roles en su tratamiento, limitación del uso y tiempo de custodia, etc. Este principio exige: i) Especificación de las finalidades: la finalidad de la captación, tratamiento, conservación y cesión de datos personales debe ser comunicada a su titular y consentida. Esa finalidad deberá ser clara, específica y significativa, a la vista de las circunstancias; ii) Minimización del perímetro de la información captada, de la identificabilidad de los datos, así como de su uso, conservación y revelación.

[56] La protección de la privacidad debe estar integrada en el diseño, en la arquitectura, en el ADN de los sistemas informáticos y las prácticas empresariales. La privacidad debe dejar de tratarse como un módulo añadido a algo que ya existía o que ya funcionaba, como una medida accesoria de seguridad. Y alcanzar la categoría de elemento "core", nuclear, pero sin perjuicio de la funcionalidad del sistema. Una de las principales aportaciones de Cavoukian, es la de imponer modelos "win-win", en el que la privacidad merezca el mismo interés y esfuerzo que el objetivo empresarial o institucional del sistema diseñado. En estos casos, será preciso volver a empezar hasta conseguir que la aplicación o sistema haga lo que tenga que hacer, y la privacidad de sus usuarios o de los datos gestionados sea respetada con la misma eficacia. La consagración del Privacy by Design exige un acercamiento multidisciplinar e integral, eminentemente creativo: será preciso innovar para reinventar, a veces desde cero, un montón de realidades actuales, que desde este nuevo prisma resultan inaceptables. Además, el desarrollo o diseño respetuoso con la privacidad, debe ser demostrable. Es más, debe ser documentado y publicado a disposición de los usuarios o titulares de datos afectados: i) El funcionamiento y eficacia de los estándares y políticas aplicadas deben ser susceptibles de revisión y auditoría externa; ii) Se ejecutarán evaluaciones de impacto y análisis de riesgo en términos de privacidad. Sus resultados serán publicados, con detalle de los riesgos detectados y medidas adoptadas para mitigarlos, otras

4. Funcionalidad Total – “Todos ganan”, no “Si alguien gana, otro pierde”. Privacidad por Diseño busca acomodar todos los intereses y objetivos legítimos de una forma “ganar-ganar”, no a través de un método anticuado de “si alguien gana, otro pierde”, donde se realizan concesiones innecesarias. Privacidad por Diseño evita la hipocresía de las falsas dualidades, tales como privacidad versus seguridad, demostrando que sí es posible tener ambas al mismo tiempo[57].

5. Seguridad Extremo-a-Extremo – Protección de Ciclo de Vida Completo. Habiendo sido incrustada en el sistema antes de que el primer elemento de información haya sido recolectado, la Privacidad por Diseño

---

alternativas valoradas y descartadas con detalle de los parámetros valorados en la comparativa y elección; iii) De acuerdo con todo lo anterior, deberá ser demostrable la minimización del impacto en términos de privacidad de la tecnología, operación o sistema resultante. Es evidente que este enfoque no puede afectar sólo a los departamentos de tecnología. Debe implica, entre otros, al rango más alto de la empresa o institución que los aplique.

[57] El Privacy by Design o Privacidad desde el Diseño pretende superar las falsas dicotomías entre privacidad y seguridad, privacidad y funcionalidad, que Cavoukian califica de “suma cero”. Estos planteamientos implican un “tira y afloja” entre factores artificiosamente enfrentados, en los que invariablemente la privacidad sale perdiendo. El Privacy by Design o Privacidad desde el Diseño no supedita la plena funcionalidad o usabilidad de la aplicación o sistemas informáticos objeto a un respeto a ultranza de la privacidad. Ello significaría conservar el actual paradigma, sólo que invirtiendo los términos. El Privacy by Design o Privacidad desde el Diseño busca conseguir lo mejor de los dos mundos: sistemas cuya eficacia y funcionalidad no interfieran entre sí. En consecuencia, si el diseño del sistema, aplicación o tecnología es muy bueno consiguiendo su funcionalidad u objetivo, pero resulta deficiente en términos de privacidad, habrá que volver a empezar. No se trata de supeditar la utilidad a la privacidad, sino de diseñar y construir sistemas y prácticas en los que ambos principios se desarrollen plenamente. Para el Privacy by Design un sistema, una app, serán plenamente funcionales (cualquiera que sea su objetivo, siempre que sea legítimo) y a la vez, plenamente respetuosos con la privacidad de sus usuarios, o no serán nada. Todos los intereses en juego y objetivos perseguidos serán documentados desde el principio del diseño: se plantearán (y evitarán) negociaciones de “suma cero” en favor de soluciones que permitan la funcionalidad de todos los objetivos perseguidos. Nadie dice que esto sea fácil. Pero es posible. Y el premio para el que lo consiga es doble: i) La entidad que aplique con éxito demostrable este principio, cumplirá con las obligaciones de accountability (responsabilidad proactiva en el cumplimiento -y capacidad de prueba de dicho cumplimiento- de las obligaciones de aseguramiento de datos personales). Podrá mostrar una posición sólida frente a la administración, si se ve involucrada en un incumplimiento o brecha de seguridad. Atendiendo a las circunstancias, podrá exonerarse o en todo caso mitigar la responsabilidad en la que pueda haber incurrido; ii) Por otra parte conseguirá, frente al usuario y resto de players del mercado, el liderazgo en materia de privacidad, ámbito en el que el liderazgo y la confianza son hoy muy caros de conseguir.

se extiende con seguridad a través del ciclo de vida completo de los datos involucrados – las medidas de seguridad robustas son esenciales para la privacidad, de inicio a fin. Esto garantiza que todos los datos son retenidos con seguridad, y luego destruidos con seguridad al final del proceso, sin demoras. Por lo tanto, la Privacidad por Diseño garantiza una administración segura del ciclo de vida de la información, desde la cuna hasta la tumba, desde un extremo hacia el otro[58].

6. Visibilidad y Transparencia – Mantenerlo Abierto. Privacidad por Diseño busca asegurar a todos los involucrados que cualquiera que sea la práctica de negocios o tecnología involucrada, está en realidad esté operando de acuerdo a las promesas y objetivos declarados, sujeta a verificación independiente. Sus partes componentes y operaciones permanecen visibles y transparentes, a usuarios y a proveedores. Recuerde, confíe pero verifique[59].

---

[58] La privacidad integrada en el sistema desde su diseño (por tanto, mucho antes de entrar en funcionamiento, de captar datos) debe protegerse, sin solución de continuidad, durante todo el ciclo vital de esos datos. La seguridad de la información impone confidencialidad, integridad, disponibilidad y resiliencia de los datos, del sistema que los cobija. Las herramientas básicas a estos efectos son la seudonimización temprana y la encriptación de datos por defecto y end to end. La encriptación exige el uso (e implementación eficaz) de un estándar suficiente de cifrado, la custodia segura de las claves de encriptación, la autenticación segura de usuarios y la imposibilidad para los usuarios de crear datos no encriptados. En consecuencia, debe asegurarse una custodia segura, un período de conservación adecuado y una destrucción asimismo segura. Estas medidas son el complemento perfecto del principio de minimización de datos (minimización del perímetro de recogida, extensión del tratamiento, tiempo de custodia y ámbito de revelación) de los datos tratados. El estándar de seguridad implicará el uso de protocolos sólidos de encriptación, destrucción, acceso y registro. Las empresas asumirán responsabilidad sobre los fallos de seguridad de la información personal, y sobre los daños causados a sus titulares.

[59] La visibilidad y transparencia son claves para establecer, por una parte, la diligencia en la protección de la privacidad ante la administración inspectora; y por otra, la confianza de los usuarios, los titulares de los datos protegidos. La publicación de las políticas aplicadas, las acciones anudadas a las mismas, de sus resultados demostrables, de las auditorías realizadas, son fundamentales para edificar la confianza de los usuarios actuales y futuros. La demostración de la aplicación preventiva de la diligencia debida en materia de seguridad y privacidad será fundamental para mitigar la responsabilidad de una empresa en supuestos de "data-breach", de filtración de datos. De acuerdo con el Privacy by Design, las instituciones deben crear un canal de comunicación con el resto de players en el ecosistema, pero sobre todo con el usuario final. Este vínculo con el usuario es clave para crear y afirmar el vínculo de confianza con él, vínculo que, en definitiva, marcará la ventaja competitiva de

7. Respeto por la Privacidad de los Usuarios – Mantener un Enfoque Centrado en el Usuario. Por encima de todo, la Privacidad por Diseño requiere que los arquitectos y operadores mantengan en una posición superior los intereses de las personas, ofreciendo medidas tales como predefinidos de privacidad robustos, notificación apropiada, y facultando opciones amigables para el usuario. Hay que mantener al usuario en el centro de las prioridades[60]».

---

las empresas líderes en privacidad sobre el resto. A estos efectos, es importante conseguir que el usuario tenga herramientas para acceder a sus datos objeto de tratamiento, controlarlos (ejerciendo sus derechos sobre los mismos: revocación, limitación, olvido, portabilidad, reclamación, etc…). Estas herramientas estarán disponibles online y en tiempo real, si es posible. El usuario debe recibir información en términos claros e inteligibles (y no incomprensibles e interminables textos de términos y condiciones, bajo el actual paradigma "son lentejas"). Los usuarios, pero también el resto de partes interesadas, podrán asegurarse de que la tecnología y/o el negocio se conducen de conformidad con los objetivos y compromisos anteriores. Esta conformidad estará sujeta a verificación independiente. La recogida de datos personales trae consigo una lógica responsabilidad sobre su custodia. Las políticas de privacidad se documentarán y publicarán, y se trasladarán contractualmente en cascada a los terceros cesionarios de datos personales. La información sobre políticas y prácticas en materia de gestión de datos personales serán públicas y estarán específicamente disponibles para sus titulares. Se establecerán mecanismos de comunicación, reclamación y compensación para los usuarios/titulares de datos.

[60] El Privacy by Design o Privacidad desde el Diseño sitúa los cimientos de la protección de la privacidad en el adecuado diseño y preconfiguración por defecto de los sistemas. Pero alcanza (hete aquí lo importante) su cima en el empoderamiento al usuario. El planteamiento "el usuario en el centro" exige diseñar con el usuario en la mente, anticipando y satisfaciendo sus inquietudes, necesidades, además de la consabida configuración (por defecto) en materia de privacidad. El usuario debe tener un papel activo y central en la gestión de sus propios datos. Y en el control de la gestión que otros hagan de los mismos. Y debe poder ejercer ese control, si ello es posible, en tiempo real. Su inacción no debe permitir menoscabos en su privacidad: por eso la configuración por defecto será la que le garantice el máximo nivel de protección. Se introduce el concepto del Control Distribuido: quizá la medida de seguridad más importante y efectiva contra abusos e incumplimientos en materia de privacidad pasa por atribuir un papel activo en la gestión (y por tanto, control) a los usuarios sobre sus propios datos. La posibilidad de chequeo individual y colectivo de los usarios sobre la gestión realizadas por terceros sobre sus datos, habilitada por el principio de visibilidad y transparencia, es seguramente el control más efectivo posible contra abusos. Garantía de una configuración de privacidad sólida y por defecto. Consentimiento libre y específico: Cuanto más sensibles sean los datos personales tratados, más claro y específico debe ser el consentimiento del titular (y por tanto, la información que le sea suministrada a tal efecto sobre la finalidad de su uso). Calidad de la información tratada: la información debe ser correcta, completa y actualizada. Acceso: Los titulares tendrán acceso a sus datos personales, y serán informados de los tratamientos y cesiones efectuadas

El conjunto de estos siete principios esenciales del concepto de *Privacy by Design* conforman la esencia del mismo, siendo un concepto fundamentalmente basado en la prevención, y en ningún caso en la corrección, ni actuando como respuesta o reacción, al adoptar siempre un carácter proactivo.

Algunos autores subrayan el hecho de que la inclusión de la protección de la privacidad en productos y servicios se realiza en la fase de diseño, y no con posterioridad a ningún hecho que pueda producirse, lo cual guarda una importante relación con el hecho del reconocimiento del poder creciente de la tecnología, capaz de implantar políticas a través de la arquitectura, la configuración y los parámetros por defecto[61].

Además, la protección que el concepto de Privacy by Design proporciona a los datos personales actúa durante todo el ciclo de vida de la información y es visible y accesible gracias a una transparencia y visibilidad reforzadas. Mediante la aplicación del concepto Privacy by Design, la protección de la privacidad está literalmente «incrustada» en el diseño de toda tecnología y además está fundamentada en un enfoque centrado en el usuario de la aplicación o del dispositivo. La idea que subyace de este concepto es que su aplicación beneficia a todos los actores implicados y literalmente, «todos ganan[62]», teniendo por objetivo hacer que todos los intereses y objetivos legítimos sean tenidos en consideración.

Por otro lado, es importante resaltar esta idea de protección durante todo el ciclo de vida de las informaciones de carácter personal, mediante la

---

sobre ellos. Y de las políticas de gestión aplicadas sobre los mismos. Cumplimiento: Se establecerán mecanismos de comunicación, reclamación y compensación a titulares de los datos

61. Mulligan, D. K. y King, J. (2012). Bridging the gap between privacy and design. *University of Pennsylvania Journal of Constitutional Law*, *14, Issue 4*, p. 992 http://ssrn.com/abstract=2070401

62 La idea de que todos los actores que tienen algo que decir en lo relativo a la concepción y desarrollo tecnológico, así como respecto a cuestiones éticas, jurídicas y de otra naturaleza que se pudieran plantear, puedan sentarse en la misma mesa, puede ser un elemento que garantice el hecho de que todos ganen y nadie pierda en el contexto de la puesta en funcionamiento de una nueva tecnología.

presencia del concepto de Privacy by Design y en la gestión de las tecnologías y sistemas[63].

Para algunos autores, el concepto de Privacy by Design puede ser catalogado de «amorphous concept»[64], pudiendo tener dos concepciones, siendo una de ellas la implementación de *Fair Information Practice Principles*[65], en el diseño y en el funcionamiento de productos y servicios que recogen o tratan de algún modo datos personales. Para lograr esto, se debe recurrir al uso de Privacy Enhancing Technologies o PET[66] existentes o crear nuevas en respuesta a las cuestiones de privacidad emergentes.

---

[63] Así se establece en la Resolución sobre Privacidad desde el Diseño (2010). XXXII Conferencia Internacional de Autoridades de Protección de Datos, de 27-29 de octubre de 2010. «Privacy by Design refers to the philosophy and approach embedding privacy into design, operation and management of information technologies and systems, across the entire information life cycle». Disponible en https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf

[64] Rubinstein, I. (2012). Regulationg Privacy by Design, *Berkeley Technological Law Journal, 26*, *p. 1421*. Recuperado de: http://ssrn.com/abstract=1837862

[65] The FIPPs are a set of five principles that are rooted in the tenets of the Privacy Act of 1974. (Privacy Act of 1974, 5 U.S.C. § 552a) cuyo texto se encuentra accesible en http://www.gpo.gov/fdsys/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf «Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information -- their "information practices" -- and the safeguards required to assure those practices are fair and provide adequate privacy protection. The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices. Common to all of these documents [hereinafter referred to as "fair information practice codes"] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress». Disponible en el siguiente link: https://web.archive.org/web/20090331134113/http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[66] Una definición de lo que ha de entenderse por estas medidas la encontramos en la Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) COM(2007) 228 final, de 2 de mayo de 2007. De este modo, «se entiende por PET un sistema coherente de medidas de TIC que protege el derecho a la intimidad suprimiendo o reduciendo los datos personales o evitando el tratamiento innecesario o indeseado de datos personales, sin menoscabo de la funcionalidad del sistema de información. La aplicación de PET puede ayudar a diseñar sistemas y servicios de información y comunicación que reduzcan al mínimo la recogida y el empleo de datos personales y faciliten el cumplimiento de la normativa sobre protección de datos». El uso de estas medidas aumentaría la confianza de los consumidores. Los usuarios tendrían la certeza de que los datos que

Pero también debe tenerse en cuenta una segunda concepción alternativa del concepto de Privacy by Design que hace referencia a la adopción de procesos, sistemas, procedimientos y políticas, las cuales pueden tener también una dimensión tecnológica, y que pueden constituir garantías o medidas protectoras de la privacidad[67].

Este concepto encierra una cierta complejidad al implicar su aplicación en tres ámbitos: «i) en los sistemas de tecnologías de la información; ii) en las prácticas de negocios responsables; y iii) en el diseño físico e infraestructura de red».[68]

El concepto de Privacy by Default integrado en el sistema, garantiza que, aunque los titulares de los datos personales no emprendan ningún tipo de acción para proteger sus datos el sistema por su propia arquitectura basada en la privacidad, va a garantizar la confidencialidad de toda información de carácter personal.

3.2 Su regulación en el RGPD

Ya la Directiva 95/46/CE incluía el riesgo como criterio para determinar las medidas técnicas y de organización apropiadas a adoptar e implementar por parte de los responsables del tratamiento[69]. La adopción de medidas se

---

facilitan para identificarse, recibir servicios o efectuar pagos sólo se emplean para fines legítimos, y de que pueden utilizar los medios informáticos sin tener que sacrificar sus derechos. La Comisión aboga por el desarrollo y mayor utilización de las PET, en particular cuando se traten datos personales en las redes de TIC. La Comisión considera que la difusión del uso de las PET incrementará la protección de la intimidad. Accesible en el siguiente link http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52007DC0228&from=ES

[67] Rubinstein, I. (2012). Regulationg Privacy by Design, *Berkeley Technological Law Journal, 26*, p. 1422. Recuperado de: http://ssrn.com/abstract=1837862

[68] Véase al respecto Cavoukian, A. (2011). Privacy by Design. Los 7 principios fundamentales, p. 1. Recuperado de. https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf

[69] Así, el Considerando 46 de la Directiva 95/46/CE declara « Considerando que la protección de los derechos y libertades de los interesados en lo que respecta a los tratamientos de datos personales exige la adopción de medidas técnicas y de organización apropiadas, tanto en el momento de la concepción del sistema de tratamiento como en el de la aplicación de los tratamientos mismos, sobre todo con objeto de garantizar la seguridad e impedir, por tanto, todo tratamiento no autorizado; que corresponde

debía hacer en dos momentos, por un lado, en el momento de la concepción del sistema de tratamiento, y por otro, en el de la aplicación de los tratamientos mismos, lo que pone de manifiesto la interrelación existente entre el riesgo y los principios de Privacy by Desing y Privacy by Default. De igual modo, se debe tener presente que «determinados tratamientos pueden presentar riesgos particulares desde el punto de vista de los derechos y las libertades de los interesados, ya sea por su naturaleza, su alcance o su finalidad»[70].

3.2.1 Protección de datos desde el diseño

El artículo 25.1 del RGPD establece el principio de la protección de datos desde el diseño:

> *«Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización[71], concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin*

---

a los Estados miembros velar por que los responsables del tratamiento respeten dichas medidas; que esas medidas deberán garantizar un nivel de seguridad adecuado teniendo en cuenta el estado de la técnica y el coste de su aplicación en relación con los riesgos que presente el tratamiento y con la naturaleza de los datos que deban protegerse;

[70] Véase el Considerando 53 de la Directiva 95/46/CE.

[71] Podemos definir la seudonimización como aquella operación que da lugar a una categoría intermedia de datos que se situaría entre los datos personales y los datos anónimos. Esta operación comporta un tratamiento de los datos personales de manera que ya no puedan atribuirse a un interesado sin utilizar otra información adicional, siempre que dicha información figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos no se atribuyen a una persona física identificada o identificable.

de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados».

En este apartado, el RGPD establece un escenario en el cual la protección que se aplica con el principio de protección de datos desde el diseño está determinado por el contexto, ya que según la situación concreta se aplicará dicho dispositivo que tiene por vocación prevenir la vulneración del derecho a la protección de datos. En este sentido, los factores a tener en cuenta no hacen referencia únicamente a criterios puramente tecnológicos, teniendo que evaluar exclusivamente en el caso concreto cuál es el estado de la técnica, sino que se valorará igualmente un factor económico en lo referente al coste específico de la aplicación. Se debe tener en cuenta igualmente cuál es la naturaleza, el ámbito, el contexto y los fines del tratamiento, lo que impactará de forma determinante en la aplicación de este principio. Pero además, se han de tener en cuenta los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas. Por tanto, se está introduciendo la necesidad de realizar un análisis de riesgos[72] que deberán ser evaluados para cada caso concreto.

El análisis que lleva a determinar si el principio de protección de datos desde el diseño es aplicable y cómo será de aplicación, está fuertemente condicionado por la existencia de riesgos en lo relativo a la protección de los datos, pero igualmente en función del grado de sensibilidad de los datos objeto del tratamiento.

El Grupo de Trabajo del artículo 29 señala que la metodología basada en el análisis de riesgos también aparecía ya en el Proyecto del RGPD como

---

[72] Afirma el Grupo del artículo 29 que con ello se introduce un enfoque denominado Risk-based approach. Véase al respecto el Dictamen *Statement on the role of a risk-based approach in data protection legal frameworks*, WP 218, de 30 de mayo de 2014, p.2. Esta metodología que se basa en la noción de riesgo está en la base del propio RGPD y se ha visto reflejada en muchas de las medidas en el contexto de la protección de datos que recoge este texto europeo, como en los principios de protección de datos desde el diseño y por defecto, o en las evaluaciones de impacto relativas a la protección de datos que constituyen herramientas fundamentales en la identificación y valoración de los riesgos. Disponible http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf.

elemento principal de la «accountability», pero la encontramos igualmente presente en las disposiciones relativas a la obligación de seguridad o en la obligación de realizar evaluaciones de impacto en la protección de datos[73].

El RGPD nombra de forma precisa una de estas medidas, ya que hace referencia a la técnica de la seudonimización[74] con el objetivo de aplicar de forma efectiva los principios de protección de datos. Esta técnica:

> *«…consiste en la sustitución de un atributo (normalmente un atributo único) por otro en un registro. Por consiguiente, sigue existiendo una alta probabilidad de identificar a la persona física de manera indirecta; en otras palabras, el uso exclusivo de la seudonimización no garantiza un conjunto de datos anónimo […] La seudonimización reduce la vinculabilidad de un conjunto de datos con la identidad del interesado; se trata, por tanto, de una medida de seguridad útil, pero no es un método de anonimización».*[75]

Sin embargo, es innegable la importancia que esta técnica puede tener en un contexto de tratamiento masivo de datos generalizado, ya que puede representar un contrapeso importante a los riesgos que se identifican en el contexto de estos tratamientos. En todo caso, tanto esta técnica como otras pueden resultar de gran ayuda para que se puedan proteger los datos de

---

[73] Véase Id.

[74] En el Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, WP 191, de 23 de marzo de 2012, p. 11, el Grupo del artículo 29 viene declarando que «este concepto de utilización de pseudónimos debe introducirse de modo más explícito en el instrumento (por ejemplo, incluyendo una definición sobre datos bajo pseudónimo, acorde con la definición de datos personales), pues ello puede contribuir a lograr una mejor protección de datos en el contexto, por ejemplo, de la protección de datos por diseño o por defecto. Por ello, el Grupo de Trabajo sugiere que se introduzca una obligación general de anonimato o de utilización de pseudónimos para los datos personales siempre que ello sea posible y proporcionado con arreglo al objetivo del tratamiento». El texto completo puede consultarse en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp191_es.pdf

[75] Véase el Dictamen 05/2014 del Grupo del artículo 29, sobre técnicas de anonimización, 10 de abril de 2014, p. 22. El texto completo se puede consultaren http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

forma efectiva, sin frenar el desarrollo de soluciones tecnológicas basadas en el tratamiento de datos.

El artículo 25 del RGPD ha recogido esta técnica con el objetivo de contribuir a proteger «en el contexto» y con arreglo al principio a la protección de datos desde el diseño en función del objetivo del tratamiento. El legislador europeo en este mismo texto menciona de forma expresa que el uso de técnicas como puede ser esta, puede contribuir al debido cumplimiento del principio específico de la minimización de datos.

El RGPD apunta directamente a la aplicación de la protección de los datos desde el diseño teniendo en cuenta varios criterios que apuntan a una aplicación para aquellos tratamientos que por sus características específicas relativas a su «naturaleza, ámbito, contexto y fines» así como a los «riesgos de diversa probabilidad y gravedad» pueden verse originados por el mismo.

El Reglamento establece que *a priori*, son ciertos tratamientos los que necesitan de una protección específica basada en el diseño, y en particular, aquellos que presenten un riesgo que necesite de esta protección que refuerza los mecanismos ya existentes en el Reglamento.

Si analizamos cómo se ha configurado en el pasado el concepto de Privacy by Design, comprobamos que, si bien el mismo puede ser aplicado a todo tipo de dato personal, debe ser aplicado con mayor rigor a ciertos datos que presentan una especial sensibilidad. El Reglamento sigue esta orientación ya que deja la puerta abierta a que, en función de los diversos factores señalados, y tras un análisis de riesgos relativos al tratamiento se pueda determinar en qué medida este principio debe ser aplicado.

3.2.2 Protección de datos por defecto

El RGPD ha abordado el concepto de la Protección de datos por defecto de manera específica. Su artículo 25.2 establece:

> *«El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.*

Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizaran en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas».

El RGPD establece la obligación de aplicar el principio de protección de datos por defecto, haciendo hincapié en medidas que tienen por objetivo que el principio de la minimización de los datos sea respetado, ya que únicamente deberán ser tratados los datos estrictamente necesarios para el cumplimiento de las finalidades específicas del tratamiento. La protección por defecto acordada a los mismos se extiende durante todo su ciclo de vida ya que se especifica que se aplica a la cantidad de datos recogidos, a la extensión del tratamiento en cuestión, pero igualmente a su plazo de conservación y de forma particular a la accesibilidad de los mismos, ya que no deben poder acceder a los mismos un número indeterminado de personas sin la intervención de la persona.

El objetivo pretendido por parte del RGPD con este artículo, es la adopción de unos parámetros por defecto que protejan lo máximo posible los datos personales, de forma que ningún titular de los datos pueda por defecto verse expuesto a diferentes riesgos que ignora o que no sabe valorar en su justa medida.[76] En cierto modo, sería una nueva aplicación del principio de

[76] Poullet, Y. (2005). Pour une troisième generation de réglementations de protection des données. *Jusletter, 3*., p. 12. «[Rz 75] Ainsi, il s´agit pour lui de pouvoir intervenir en cas de développements technologiques présentant des risques majeurs. Ce principe dit de «précaution» largement connu en droit de l´environnement pourrait trouver à s´appliquer en matière de protection des données. Au nom de ce principe de précaution, il apparaît d´ailleurs comme nécessaire que les équipements terminaux de télécommunication (en ce compris les logiciels qui les animent) adoptent le paramétrage par défaut le plus protecteur possible, de manière à ce que la personne concernée ne puisse pas, par défaut, être exposée à divers risques qu´elle ignore ou qu´elle ne sait mesurer». Recuperado de: http://jusletter.weblaw.ch/fr/juslissues/2005/345.html

precaución en el ámbito del derecho a la protección de los datos personales cuando ciertos desarrollos tecnológicos presentan riesgos importantes[77].

3.3 Medidas concretas para la observancia de estos principios por los responsables del tratamiento y por los productores de servicios, aplicaciones y productos

3.3.1 Mecanismos de certificación en el RGPD

El artículo 25.3 RGPD establece:

> *«Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo»[78].*

---

[77] Véase al respecto Poullet, Y.: op. cit. Este autor pone como ejemplo la Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, de 23 de febrero de 1999, del Grupo del artículo 29. En concreto, su apartado tercero declara expresamente «3. La configuración de los productos informáticos (hardware y software) no debería, por defecto, permitir la recopilación, almacenado o envío de información persistente del cliente. Por ejemplo: - El software navegador debería, por defecto, estar configurado de tal forma que sólo pudiera tratarse la mínima cantidad de información necesaria para establecer una conexión Internet. Las cookies deberían, por defecto, no ser enviados ni almacenados. - Durante su instalación, una función del navegador concebida para almacenar y enviar datos sobre la identidad o el comportamiento comunicativo del usuario (perfil) no debería rellenarse automáticamente con datos previamente almacenados en el equipo informático del usuario». El Grupo del Artículo 29 incide en que, por defecto, las tecnologías deben proteger los datos personales en cuestión, impidiendo ciertas prácticas que puedan poder en riesgo dichas informaciones.

[78] El artículo 42 RGPD relativo a la certificación, establece expresamente que: «1. Los Estados miembros, las autoridades de control, el Comité y la Comisión promoverán, en particular a nivel de la Unión, la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento de lo dispuesto en el presente Reglamento en las operaciones de tratamiento de los responsables y los encargados. Se tendrán en cuenta las necesidades específicas de las microempresas y las pequeñas y medianas empresas. 2. Además de la adhesión de los responsables o encargados del tratamiento sujetos al presente Reglamento, podrán establecerse mecanismos de certificación, sellos o marcas de protección de datos aprobados de conformidad con el apartado 5, con objeto de demostrar la existencia de garantías adecuadas ofrecidas por los responsables o encargados no sujetos al presente Reglamento con arreglo al artículo 3 en el marco de transferencias de datos personales a terceros países u organizaciones internacionales a tenor del artículo 46, apartado 2, letra f). Dichos responsables o encargados deberán

Puede resultar complicado determinar si se están llevando a cabo las medidas necesarias para dar cumplimiento a estos dos principios, por lo que la certificación puede contribuir a establecer unos parámetros claros y uniformes.

El artículo 42 RGPD establece que pueden ser dos los actores que pueden ver acreditado el cumplimiento de las obligaciones que recoge el Reglamento: el responsable y el encargado del tratamiento.

Por otro lado, ya hemos comprobado cómo las obligaciones de los dos primeros párrafos del artículo 25 son de obligado cumplimiento para el responsable del tratamiento. Debemos analizar el alcance de las obligaciones que comporta el respeto de los principios de protección de datos desde el diseño y por defecto para otros actores. De igual manera, el Considerando 78[79] del RGPD hace mención al responsable y a aquellos que desarrollan productos, servicios y aplicaciones.

---

asumir compromisos vinculantes y exigibles, por vía contractual o mediante otros instrumentos jurídicamente vinculantes, para aplicar dichas garantías adecuadas, incluidas las relativas a los derechos de los interesados. 3. La certificación será voluntaria y estará disponible a través de un proceso transparente. 4. La certificación a que se refiere el presente artículo no limitará la responsabilidad del responsable o encargado del tratamiento en cuanto al cumplimiento del presente Reglamento y se entenderá sin perjuicio de las funciones y los poderes de las autoridades de control que sean competentes en virtud del artículo 55 o 56. 5. La certificación en virtud del presente artículo será expedida por los organismos de certificación a que se refiere el artículo 43 o por la autoridad de control competente, sobre la base de los criterios aprobados por dicha autoridad de conformidad con el artículo 58, apartado 3, o por el Comité de conformidad con el artículo 63. Cuando los criterios sean aprobados por el Comité, esto podrá dar lugar a una certificación común: el Sello Europeo de Protección de Datos. 6. Los responsables o encargados que sometan su tratamiento al mecanismo de certificación dará al organismo de certificación mencionado en el artículo 43, o en su caso a la autoridad de control competente, toda la información y acceso a sus actividades de tratamiento que necesite para llevar a cabo el procedimiento de certificación. 7. La certificación se expedirá a un responsable o encargado de tratamiento por un período máximo de tres años y podrá ser renovada en las mismas condiciones, siempre y cuando se sigan cumpliendo los requisitos pertinentes. La certificación será retirada, cuando proceda, por los organismos de certificación a que se refiere el artículo 43, o en su caso por la autoridad de control competente, cuando no se cumplan o se hayan dejado de cumplir los requisitos para la certificación. 8. El Comité archivará en un registro todos los mecanismos de certificación y sellos y marcas de protección de datos y los pondrá a disposición pública por cualquier medio apropiado».

[79] En concreto, el Considerando 78 RGPD afirma que «La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas

Así, comprobamos cómo se impone al responsable del tratamiento la adopción de políticas internas y la aplicación de medidas para el cumplimiento de los principios de protección de datos desde el diseño y por defecto. Además de la seudonimización, se enumeran otras medidas que conducen al cumplimiento de estos principios, como son la reducción al máximo el tratamiento de datos personales y el dar transparencia a las funciones y al tratamiento de los datos, lo que conllevaría por un lado permitir a los interesados supervisar el tratamiento de sus datos y, por otro, que el responsable del tratamiento pueda crear y mejorar elementos de seguridad.

Este listado no es exhaustivo, el mismo Considerando 78 RGPD recoge explícitamente la expresión «entre otras». De este modo, se ofrece una orientación sobre cuáles son las acciones a llevar a cabo para respetar los principios de protección de datos por diseño y por defecto. Además, se identifican dos ámbitos que pueden tener un impacto importante en estos principios de protección de datos señalados. Nos referimos al principio de minimización de datos y la obligación de transparencia.

Ahora bien, se ha de tener en cuenta que la concepción o el diseño de los sistemas de tratamientos de datos está en muchas ocasiones en manos de los diseñadores de productos o de software, y no tanto en manos de los

---

técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos».

responsables del tratamiento[80]. A lo largo de todo el procedimiento de elaboración del RGPD, se ha apostado por la inclusión de los productores de los productos, servicios y aplicaciones, como terceros intervinientes que han de tener en cuenta el derecho de protección de datos, cuando desarrollen y diseñen estos productos, servicios y aplicaciones. Atendiendo a esta finalidad, se estableció expresamente por parte del Consejo de la Unión Europea en el Considerando 61[81] de su Propuesta RGPD, una llamada de atención sobre la necesidad de alentar la aplicación de los principios de la protección desde el diseño y por defecto por parte de los desarrolladores de tecnologías.

---

[80]Commission de la Protection de la vie Privée, Avis n° 35/2012 du 21 novembre 2012 d'initiative sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractè e personnel et à la libre circulation de ces données1 (CO-A-2012-015), Belgique. «87. La CPVP soutient l'insertion de ces principes mais souligne le fait que la conception des systèmes de traitement est parfois dans les mains, non pas des responsables de traitement, mais plutôt des concepteurs de produits ou de logiciels».El texto completo puede consultarse en el link: https://www.privacycommission.be/sites/privacycommission/files/documents/avis_35_2012_0.pdf

[81] Consejo de la Unión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) - Preparación de un planteamiento general, 11 de junio de 2015. «61) La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de las oportunas medidas de carácter técnico y organizativo con el fin de garantizar el cumplimiento de lo dispuesto en el presente Reglamento. Con objeto de poder demostrar la conformidad con lo dispuesto en el presente Reglamento, el responsable debe adoptar las políticas internas y aplicar las medidas adecuadas que cumplan especialmente los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en minimizar el tratamiento de datos personales, (…) hacer uso de seudónimos en los datos personales lo antes posible, transparencia con respecto a las funciones y al tratamiento de datos personales, permitir a los interesados supervisar el tratamiento de datos, permitir al responsable del tratamiento crear y mejorar elementos de seguridad. A la hora de desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, deberá animarse a los productores de los productos, servicios y aplicaciones a tener en cuenta el derecho a la protección de datos cuando desarrollen y diseñen estos productos, servicios y aplicaciones, y, con la debida atención al estado de la técnica, se aseguren de que los responsables y los encargados del tratamiento están en disposición de cumplir sus obligaciones en materia de protección de datos». http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf

Los cambios introducidos en la Propuesta inicial de la Comisión por el Consejo de la Unión Europea en este Considerando 61, en referencia a los productores de tecnologías, son los que finalmente han sido recogidos por el Considerando 78 del RGPD, que establece de forma precisa que ha de alentarse a los productores de productos, servicios y aplicaciones que están basados en el tratamiento de datos personales o que traten datos personales para cumplir su función, a que tengan en cuenta al derecho a la protección de datos al desarrollarlos y diseñarlos.

Igualmente señala que estos productores deben asegurarse, teniendo en cuenta el estado de la técnica, de que tanto el responsable como el encargado del tratamiento, van a poder cumplir sus obligaciones en materia de protección de datos.

La certificación, aplicada a la protección de datos personales, además de que pueda «servir de elemento para demostrar el cumplimiento»[82], ayuda a generar confianza. En concreto, la certificación da lugar a que responsables y/o encargados del tratamiento puedan, previa intervención de un tercero con la pericia, solvencia e independencia necesarias, obtener un distintivo que acredite que han sido objeto de un proceso de evaluación de conformidad en materia de protección de datos, debiendo considerarse en cada caso el alcance de la misma.

A diferencia de la Directiva 95/46/CE, en la que no se hace referencia a la certificación y a otros distintivos como los sellos y marcas de protección de datos, el nuevo marco normativo de protección de datos sí lo recoge dentro de su articulado, e incentiva la creación de mecanismos de certificación mediante los cuales, el responsable o encargado del tratamiento puedan demostrar el cumplimiento de las obligaciones que legalmente le incumben[83].

---

[82] Así, el Considerando 81 del RGPD declara que «la adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable».

[83] En concreto, el RGPD reconoce esta posibilidad tanto al responsable del tratamiento como al encargado del mismo. De este modo, por lo que se refiere a la responsabilidad del primero de ellos,

De este modo, el responsable del tratamiento puede acreditar con un sello o marca de protección de datos, que facilita al interesado las informaciones[84] y las comunicaciones tipificadas en el artículo 12 RGPD, e incluso que lo hace de un modo que es acorde con los principios de transparencia vistos anteriormente.

Su virtualidad no reside en su carácter liberatorio, pues la certificación no limita la responsabilidad del responsable y se entenderá sin perjuicio de las funciones de las autoridades de control, sino en que permite que el usuario, de un modo sencillo, e incluso automático, conozca el nivel de protección de datos de los productos y servicios que considere utilizar. Así lo reconoce el Considerando 100[85] del RGPD.

3.3.2 Apuesta por la responsabilidad proactiva en el RGPD

El derecho a indemnización de las personas físicas por los daños causados en el tratamiento ilegal de sus datos de carácter personal se regula en el artículo 82 RGPD[86]

---

el artículo 24.3 RGPD expresamente declara que «la adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento»; en relación al segundo, el artículo 28.5 RGPD afirma que «la adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo».

[84] Nos referimos al conjunto de las obligaciones tipificadas en los artículos 13 y 14 del RGPD. Este, hace una distinción atendiendo al origen de la obtención de los datos personales.

[85] El Considerando 100 RGPD expresa que «a fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes».

[86] Así, en relación al derecho a indemnización y responsabilidad, el RGPD recoge expresamente en su artículo 82 que «1. Toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción del presente Reglamento tendrá derecho a recibir del responsable o el encargado del tratamiento una indemnización por los daños y perjuicios sufridos. 2. Cualquier responsable que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente

Se trata de la primera vez que se regula en el Derecho de la Unión Europea. Con anterioridad, la Directiva 95/46/CE introdujo un mandato a los legisladores nacionales para que reconociesen el derecho a indemnización de las personas perjudicadas por el tratamiento ilícito de sus datos[87]. En España, la transposición se efectuó a través de lo dispuesto en el artículo 19 LOPD[88].

Así, cuando el responsable y/o el encargado del tratamiento de datos de carácter personal infrinjan lo dispuesto en el RGPD, y con ello causen un daño a una persona física, éstos no solo podrán ser sancionados por su acción u omisión, sino que además, podrán ser declarados responsables de

---

Reglamento. Un encargado únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable. 3. El responsable o encargado del tratamiento estará exento de responsabilidad en virtud del apartado 2 si demuestra que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios. 4. Cuando más de un responsable o encargado del tratamiento, o un responsable y un encargado hayan participado en la misma operación de tratamiento y sean, con arreglo a los apartados 2 y 3, responsables de cualquier daño o perjuicio causado por dicho tratamiento, cada responsable o encargado será considerado responsable de todos los daños y perjuicios, a fin de garantizar la indemnización efectiva del interesado. 5. Cuando, de conformidad con el apartado 4, un responsable o encargado del tratamiento haya pagado una indemnización total por el perjuicio ocasionado, dicho responsable o encargado tendrá derecho a reclamar a los demás responsables o encargados que hayan participado en esa misma operación de tratamiento la parte de la indemnización correspondiente a su parte de responsabilidad por los daños y perjuicios causados, de conformidad con las condiciones fijadas en el apartado 2. 6. Las acciones judiciales en ejercicio del derecho a indemnización se presentarán ante los tribunales competentes con arreglo al Derecho del Estado miembro que se indica en el artículo 79, apartado 2».

[87] El artículo 23 de la Directiva 95/46/CE disponía: «1. Los Estados miembros dispondrán que toda persona que sufra un perjuicio como consecuencia de un tratamiento ilícito o de una acción incompatible con las disposiciones nacionales adoptadas en aplicación de la presente Directiva, tenga derecho a obtener del responsable del tratamiento la reparación del perjuicio sufrido. 2. El responsable del tratamiento podrá ser eximido parcial o totalmente de dicha responsabilidad si demuestra que no se le puede imputar el hecho que ha provocado el daño».

[88] En relación al derecho a indemnización, la LOPD declaraba en su artículo 19 que «1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados. 2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas. 3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria».

la lesión y, en su caso, deberán indemnizar al perjudicado. Es evidente que sendos mecanismos, la sanción administrativa a través de las correspondientes autoridades nacionales de control, y la responsabilidad civil a que se enfrentan los responsables y/o encargados de tratamientos ilícitos de datos de carácter personal, responden a diferentes finalidades: por un lado, la sanción administrativa que, como manifestación del *ius puniendi* del Estado, tiene una finalidad preventiva. Por otro lado, la institución de la acción resarcitoria del daño, de la responsabilidad civil o, en su caso, patrimonial de la Administración, tiene por finalidad resarcir al perjudicado de los daños y perjuicios sufridos por el tratamiento ilegal de sus datos[89].

En atención a lo previsto en el Considerando 11[90] del RGPD, la protección efectiva de los datos personales en la Unión exige, entre otras consideraciones, que las infracciones a las obligaciones previstas se castiguen con sanciones equivalentes (económicas o no). En definitiva, que la vulneración de este derecho fundamental no quede impune en ninguno de los Estados miembros.

Este es, precisamente, uno de los principales objetivos que se persigue con el RGPD, alcanzar una armonización que impida la existencia de regulaciones dispares. En este sentido, no podemos dejar al margen que una de las principales críticas sobre la Directiva 95/46/CE se refería a la excesiva libertad con la que contaban los Estados miembros a la hora de establecer el correspondiente régimen sancionador[91], de manera que el

---

[89] Véase, entre otros, de Palma del Teso, A. (1996) El principio de culpabilidad en el derecho administrativo sancionador. Madrid: Tecnos, pp. 43 y 46 a 51.

[90] El Considerando 11 declara expresamente que «la protección efectiva de los datos personales en la Unión exige que se refuercen y especifiquen los derechos de los interesados y las obligaciones de quienes tratan y determinan el tratamiento de los datos de carácter personal, y que en los Estados miembros se reconozcan poderes equivalentes para supervisar y garantizar el cumplimiento de las normas relativas a la protección de los datos de carácter personal y las infracciones se castiguen con sanciones equivalentes».

[91] Conforme podemos apreciar en el artículo 24 de la Directiva 95/46/CE, se dejaba un amplio margen de apreciación a los Estados miembros sobre el régimen sancionador. «Los Estados miembros adoptarán las medidas adecuadas para garantizar la plena aplicación de las disposiciones de la

tratamiento de las infracciones y sanciones podía variar radicalmente de un Estado a otro[92], como de hecho ocurría.

En el mismo sentido se pronuncia el RGPD en su Considerando 148, al indicar que

> *«…cualquier infracción debe ser castigada con sanciones, incluidas multas administrativas, con carácter adicional a medidas adecuadas impuestas por la autoridad de control en virtud del presente Reglamento, o en sustitución de estas».*

Lo que se pretende con el RGPD, como medida fundamental de armonización, es que todas las autoridades de control[93] puedan imponer multas administrativas por la comisión de infracciones, de manera que se eviten los denominados «paraísos de datos»[94] dentro de la Unión Europea que, de alguna manera, impidan la libre circulación de los datos, obstaculicen el ejercicio de las actividades económicas y falseen la competencia, impidiendo que las autoridades cumplan las funciones encomendadas por el Derecho de la Unión[95].

---

presente Directiva y determinarán, en particular, las sanciones que deben aplicarse en caso de incumplimiento de las disposiciones adoptadas en ejecución de la presente Directiva».

[92] En este sentido puede verse el «Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE), [COM (2003) 265 final], Bruselas 15.05.2003» http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52003DC0265&from=ES

[93] Véase al respecto el Considerando 150 RGPD: «a fin de reforzar y armonizar las sanciones administrativas por infracción del presente Reglamento, cada autoridad de control debe estar facultada para imponer multas administrativas».

[94] Con esta denominación, se pretende hacer referencia a aquellos países que cuentan con una legislación más laxa en materia de protección de datos, o cuya aplicación es menos eficaz, de manera que las empresas deciden instalar sus sedes o filiales para no estar sometidas a un régimen demasiado estricto.

[95] Así lo manifiesta expresamente el Considerando 9 del RGPD: «Aunque los objetivos y principios de la Directiva 95/46/CE siguen siendo válidos, ello no ha impedido que la protección de los datos en el territorio de la Unión se aplique de manera fragmentada, ni la inseguridad jurídica ni una percepción generalizada entre la opinión pública de que existen riesgos importantes para la protección de las personas físicas, en particular en relación con las actividades en línea. Las diferencias en el nivel de protección de los derechos y libertades de las personas físicas, en particular del derecho a la protección

No obstante, el RGPD no agota toda la regulación del régimen sancionador, sino que en determinados aspectos deja cierto margen, más o menos amplio, a los Estados para que completen con su propia normativa interna.

Junto con el artículo 83 RGPD, que establece las condiciones generales para la imposición de multas administrativas, el artículo 84 del mismo texto legal prevé que los Estados puedan imponer otro tipo de sanciones distintas a las multas administrativas[96]. Por tanto, podemos deducir que existen dos tipos de sanciones por la comisión de las correspondientes infracciones:

En primer lugar, sanciones económicas, denominadas por el propio RGPD «multas administrativas», para las infracciones previstas en el artículo 83, que son la gran mayoría. En este caso, la regulación es muy detallada, y no se deja margen alguno a los Estados para regular más allá de los que establece el propio RGPD. Además, este tipo de multas tendrán carácter adicional o sustitutivo de las medidas contempladas en el artículo 58.2 RGPD[97].

---

de los datos de carácter personal, en lo que respecta al tratamiento de dichos datos en los Estados miembros pueden impedir la libre circulación de los datos de carácter personal en la Unión. Estas diferencias pueden constituir, por lo tanto, un obstáculo al ejercicio de las actividades económicas a nivel de la Unión, falsear la competencia e impedir que las autoridades cumplan las funciones que les incumben en virtud del Derecho de la Unión. Esta diferencia en los niveles de protección se debe a la existencia de divergencias en la ejecución y aplicación de la Directiva 95/46/CE».

[96] Expresamente, el apartado primero del artículo 84 RGPD establece: «los Estados miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del presente Reglamento, en particular las infracciones que no se sancionen con multas administrativas de conformidad con el artículo 83, y adoptarán todas las medidas necesarias para garantizar su observancia. Dichas sanciones serán efectivas, proporcionadas y disuasorias».

[97] A este respecto, expresamente declara el apartado segundo del Artículo 58 «2.Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: a) sancionar a todo responsable o encargado del tratamiento con una advertencia cuando las operaciones de tratamiento previstas puedan infringir lo dispuesto en el presente Reglamento; b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento; c) ordenar al responsable o encargado del tratamiento que atiendan las solicitudes de ejercicio de los derechos del interesado en virtud del presente Reglamento; d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado; e) ordenar al responsable del tratamiento que comunique al interesado las violaciones de la seguridad de los datos personales; f) imponer una

En segundo lugar, el artículo 84 del RGPD se refiere a otro tipo de sanciones que los Estados miembros deberán establecer para aquellas infracciones que no se sanciones con multas económicas de conformidad con lo previsto en el artículo 83. Por tanto, los Estados miembros establecerán otras sanciones diferentes a las multas económicas previstas, dejándoles un amplio margen para establecer su régimen jurídico, que deberá respetar os principios de proporcionalidad y disuasión.

El ejercicio de la potestad sancionadora, para la imposición de multas administrativas, viene atribuido por el artículo 83.1 RGPD a las autoridades de control de cada Estado miembro[98]. En nuestro país será la Agencia Española de Protección de Datos quien ejerza esta potestad.

Sin embargo, respecto a las sanciones previstas en el artículo 84, el RGPD se limita a señalar que los Estados miembros establecerán las normas aplicables, sin especificar el órgano concreto que deba, en su caso, imponerlas. Considero que deberían ser igualmente las autoridades de control.

---

limitación temporal o definitiva del tratamiento, incluida su prohibición; g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19; h) retirar una certificación u ordenar al organismo de certificación que retire una certificación emitida con arreglo a los artículos 42 y 43, u ordenar al organismo de certificación que no se emita una certificación si no se cumplen o dejan de cumplirse los requisitos para la certificación; i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular; j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.

[98] Todo ello, sin perjuicio de aquellos Estados cuyo régimen constitucional reserva a los tribunales integrantes del Poder Judicial la imposición de multas económicas, pues en estos casos, el Reglamento prevé que sea la autoridad de control quien incoe el procedimiento y los tribunales nacionales quienes impongas la correspondiente sanción, que tendrá que tener un efecto equivalente a las multas administrativas impuestas por las restantes autoridades de control. Así se establece expresamente en el artículo 83.9 RGPD

3.3.2.1 Comisión de infracciones por personas físicas o jurídicas

El artículo 82.2 RGPD establece la responsabilidad del responsable del tratamiento «que participe en la operación de tratamiento responderá de los daños y perjuicios causados en caso de que dicha operación no cumpla lo dispuesto por el presente Reglamento». Es decir, se establece la responsabilidad del responsable del tratamiento cuando participe en una operación y ésta no cumpla, por acción u omisión, lo dispuesto en el Reglamento y las normas derivadas de su regulación.

Sin embargo, hemos de tener presente que el encargado del tratamiento «únicamente responderá de los daños y perjuicios causados por el tratamiento cuando no haya cumplido con las obligaciones del presente Reglamento dirigidas específicamente a los encargados o haya actuado al margen o en contra de las instrucciones legales del responsable». Ahora bien, esas obligaciones o instrucciones pueden ser fácticas, jurídicas, de acción u omisión.

En cuanto a un tratamiento que incumpla lo dispuesto en el RGPD, el legislador europeo especifica que ello incluye un tratamiento que infrinja, además de las disposiciones del RGPD, también los actos delegados y de ejecución adoptados de conformidad con el RGPD, así como las normas de los Estados miembros adoptadas en desarrollo o cumplimiento del RGPD[99].

El artículo 82 del RGPD señala al responsable y/o al encargado u encargados del tratamiento ilícito como responsables por los daños causados en la operación de tratamiento cuando el primero incumpla lo dispuesto en el RGPD, o bien el segundo incumpla las obligaciones que le impone de forma específica el RGPD o las instrucciones del responsable del tratamiento.

---

[99] Véase al respecto el Considerando 146 del RGPD: «un tratamiento en infracción del presente Reglamento también incluye aquel tratamiento que infringe actos delegados y de ejecución adoptados de conformidad con el presente Reglamento y el Derecho de los Estados miembros que especifique las normas del presente Reglamento».

El RGPD establece la responsabilidad directa del responsable del tratamiento de datos personales ilícito que cause daños a una persona física tanto si el tratamiento lo realizó in house o lo externalizó a un tercero. Este último, como encargado del tratamiento, tiene una responsabilidad más limitada, porque solo responderá por los daños causados cuando incumpla las obligaciones que le impone el RGPD y las normas derivadas del mismo, que son menores que las que corresponden al responsable del tratamiento de datos, o bien desobedezca las instrucciones que le de este último. Esta limitación de la responsabilidad del encargado del tratamiento resulta lógica, ya que no podemos olvidar que el encargado del tratamiento de datos actúa siempre por mandato del responsable del tratamiento[100].

El legislador europeo ha optado por el principio de responsabilidad subjetiva, que se aplica en todos los países de nuestro entorno incluso a los daños causados por la Administración pública[101].

---

[100] Véase Recio Gayo, M. (2015). Acerca de la evolución de la figura del encargado del tratamiento. *Revista de Privacidad y Derecho Digital*, *nº 0*.

[101] Como es sabido, el sistema español acoge el principio de responsabilidad subjetiva en Derecho civil y en Derecho penal, pero no así en Derecho Administrativo, en el que la Administración pública responde por los daños causado con su acción u omisión, con actos jurídicos o actuaciones fácticas, con independencia de que sus agentes actúen con dolo, culpa o negligencia. Es decir, se estableció la responsabilidad objetiva por funcionamiento normal o anormal de los servicios públicos. Así se recoge en los apartados primero y segundo del artículo 32 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, BOE núm. 236, de 2 de octubre, de 201, al declarar expresamente: «1. Los particulares tendrán derecho a ser indemnizados por las Administraciones Públicas correspondientes, de toda lesión que sufran en cualquiera de sus bienes y derechos, siempre que la lesión sea consecuencia del funcionamiento normal o anormal de los servicios públicos salvo en los casos de fuerza mayor o de daños que el particular tenga el deber jurídico de soportar de acuerdo con la Ley. La anulación en vía administrativa o por el orden jurisdiccional contencioso administrativo de los actos o disposiciones administrativas no presupone, por sí misma, derecho a la indemnización. 2. En todo caso, el daño alegado habrá de ser efectivo, evaluable económicamente e individualizado con relación a una persona o grupo de personas». Son numerosos los trabajos en materia de responsabilidad patrimonial de la Administración pública. Entre otros muchos, nos remitimos al autor Martín Rebollo, L. (1977). *La responsabilidad patrimonial de la Administración en la jurisprudencia*, Madrid: Civitas y Martín Rebollo, L. (2011). Fundamento y función de la responsabilidad patrimonial del Estado: situación actual y perspectivas en el derecho español. *Revista española de Derecho Administrativo*, *4*, pp. 3-40.

Así, la regulación del RGPD del derecho de indemnización resulta acorde con la responsabilidad subjetiva, por dolo, culpa o negligencia que, como he señalado, rige en los sistemas jurídicos de nuestro entorno y que, por tanto, es la aplicable para exigir la responsabilidad extracontractual de las instituciones y organismos de la Unión Europea, conforme a lo dispuesto en el segundo párrafo del artículo 340[102] del Tratado de Funcionamiento de la Unión Europea.

En este sentido, el artículo 82.3 del RGPD exonera de responsabilidad por los daños causados en la operación de tratamiento de datos de carácter personal al responsable y/o al encargado cuando demuestren «que no es en modo alguno responsable del hecho que haya causado los daños y perjuicios».

Sin embargo, dada la configuración del sistema de responsabilidad patrimonial de la Administración pública en España como un sistema de responsabilidad objetiva, cuando el responsable o encargado del tratamiento sea personal de la Administración española, el perjudicado por el tratamiento ilícito podrá, si se dan los requisitos que exige la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, ejercitar la acción de reclamación de responsabilidad patrimonial frente a dicha Administración aunque no haya dolo, culpa o negligencia en el mismo.

El legislador europeo regula, por primera vez, la necesaria indemnización de los daños causados por un tratamiento no acorde con lo dispuesto en el RGPD. Se trata por tanto de una responsabilidad por daños, con fines resarcitorios, que no deriva de un incumplimiento contractual y que, por tanto, no pretende resarcir dicho incumplimiento, sino la lesión de un derecho fundamental.

Por su parte, el artículo 83.2 RGPD opta por la modulación y graduación de las cuantías de las multas en función de circunstancias de cada caso

---

[102] Atendiendo a lo estipulado en el párrafo segundo del artículo 340 TFUE, «en materia de responsabilidad extracontractual, la Unión deberá reparar los daños causados por sus instituciones o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a los Derechos de los Estados miembros».

individual, lo que evidencia una apuesta decidida por la responsabilidad proactiva o *accountability*[103] como criterio inspirador del régimen sancionador. Esto es, a mayor proactividad del sujeto sancionado, mayor probabilidad de que se disminuya la sanción. Esta forma de entender el régimen sancionador, ya ha sido implantada en nuestro Ordenamiento a raíz de la modificación de la LOPD en al año 2011[104].

Los objetivos fundamentales que se buscan con este régimen modular de las multas, y degradador de las sanciones, es doble: i) humanizar las sanciones en supuestos en que los responsables sean personas físicas y pequeñas y medianas empresas; y ii) premiar la conducta responsable y vocacionalmente cumplidora de la legislación de protección de datos cuando se hubieran cometido infracciones sin intención, o a título de mera inobservancia, pero al mismo tiempo, se haya reaccionado con diligencia para paliar sus efectos[105].

Esta posibilidad de modular las multas administrativas que se pueden imponer parece un régimen adecuado al principio de proporcionalidad, dado el importe que pueden alcanzar las sanciones. Aunque, por otro lado, se está otorgando un amplio poder discrecional a las autoridades de control, lo que puede dar lugar distintos criterios de interpretación según el Estado miembro de que se trate, dando lugar a una fragmentación en la aplicación

---

[103] El artículo 5.2 RGPD, en relación a los principios relativos al tratamiento, declara «el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)». De igual modo, en el Considerando 85 se hace una mención expresa al mismo término «Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas».

[104] Véase al respecto Piñar Mañas, J.L. (2011). La importante reforma del régimen sancionador en materia de protección de datos: reflexiones urgentes», *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, *50.*

[105] Véase al respecto Rallo Lombarte, A. (2014). Estudios sobre la evolución del régimen sancionador en la legislación de protección de datos. *Revista de Estudios Políticos*, *166*, 2014, p.116

del Reglamento que era, precisamente, lo que se pretendía evitar, redundando, además, en un incremento de la inseguridad jurídica.

3.3.2.2 Comisión de infracciones por las Administraciones públicas. Régimen sancionador especial

Conforme se declara en el RGPD en los apartados 7 y 8 del artículo 4[106], las personas, ya sean físicas o jurídicas y las autoridades públicas pueden ser responsables o encargados del tratamiento.

Así, las Administraciones Públicas también estás sometidas a las obligaciones recogidas en el RGPD y, por consiguiente, pueden incurrir en la comisión de infracciones de acuerdo con lo previsto en su artículo 83. En el mismo sentido, nuestra legislación interna también recoge la posibilidad de la comisión de infracciones por parte de las Administraciones públicas. En concreto, la LOPD lo recoge en su artículo 46 en los siguientes términos

> *«1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera. 2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a*

---

[106] Artículo 4 RGPD. «A efectos del presente Reglamento se entenderá por: […] 7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros; 8) «encargado del tratamiento» o «encargado»:la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento».

aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas».

El apartado 1 del artículo 48 del mismo texto legal señala que el procedimiento a seguir para la determinación de las infracciones y la imposición de sanciones se establecerá por vía reglamentaria. Siguiendo estas indicaciones, el artículo 129 RLOPD señala el procedimiento a seguir para declarar la existencia de una infracción por parte de las Administraciones públicas[107].

Pues bien, tal y como se estipula en el artículo 83.7 RGPD, este régimen señalado seguirá vigente, pues expresamente[108] se deja a los Estados miembros libertad para determinar si es posible, y bajo qué circunstancias, imponer multas administrativas a las autoridades y organismos públicos establecidos en cada uno de los Estados miembros. En definitiva, la LOPD y su reglamento de desarrollo mantienen su aplicación directa en el régimen jurídico sobre la declaración de infracción que puede imponerse a las Administraciones Públicas, por vulneración de las obligaciones recogidas en el RGPD, en sustitución de las multas administrativas.

3.3.2.3 Comisión de infracciones por los organismos de certificación

La nueva regulación prevista en el RGPD viene a ampliar los sujetos pasivos de la relación jurídico-sancionadora al establecer[109] la posibilidad de

---

[107] Cuestión distinta es que, con motivo de la comisión de una infracción, aquellas no estén sometidas al régimen sancionador previsto para las personas privadas y, por tanto, no se les imponga la correspondiente multa administrativa, sino que sea suficiente con una «declaración de infracción».

[108] El Artículo 83.7 RGPD declara: «Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro».

[109] Expresamente establece el artículo 83.4 RGPD «4.Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía: a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; b) las

imponer sanciones no solo a los responsables y encargados, sino también a los organismos de certificación por la vulneración de los artículos 42 y 43 (relacionados con la certificación), y a los organismos de supervisión de los códigos de conducta por la vulneración de obligaciones a las que se refiere el apartado 4 del artículo 41 (referente a la supervisión de códigos de conducta aprobados) del propio Reglamento.

La posibilidad de sancionar a los organismos de certificación es una consecuencia lógica, habida cuenta del protagonismo que adquieren. Con la nueva regulación, estos organismos asumen funciones muy relevantes en relación a la certificación del cumplimiento de las obligaciones establecidas en el Reglamento por parte de los responsables y encargados y, por tanto, adquieren altas dosis de responsabilidad. Lo mismo cabe decir en relación a los organismos que supervisan el cumplimiento de los correspondientes códigos de conducta.

3.4 Transparencia y Protección de datos desde el diseño

El principio de protección de datos desde el diseño, puede resultar altamente eficiente desde el punto de vista de la transparencia[110]. Con anterioridad, se ha podido apreciar cómo, entre las herramientas básicas para encauzar de modo adecuado los conflictos entre privacidad y transparencia, se encuentra el análisis de los riesgos asociados a este conflicto.

No obstante, afirma MARTÍNEZ MARTÍNEZ que esta tarea no debería limitarse a una mera ponderación objetiva de los derechos en conflicto. Es perfectamente posible otro enfoque basado en la metodología de desarrollo de la documentación. En esta aproximación, la cuestión a dilucidar no sería tanto qué derecho prevalece, sino cómo podemos ser capaces de generar la información de modo tal que permita una anonimización eficiente, o el

---

obligaciones de los organismos de certificación a tenor de los artículos 42 y 43; c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4».

[110] Valero Torrijos, J. (2013). *Derecho, innovación y Administración electrónica*. Sevilla: Derecho Global.

acceso parcial al que se refiere el artículo 16 LTBG[111]. Debemos contemplar los referentes históricos en el camino de la consolidación del diseño basado, o respetuoso con la privacidad. La preocupación por el intercambio de información personal en Internet y las trabas procedimentales que ello suponía en procesos de suscripción dio lugar a finales de los noventa a la propuesta de las Privacy Enhancing Technologies (PET) y la Plattform for Privacy Preferences (P3P). La idea que alumbra estos proyectos es que, si un programador actúa materialmente como un regulador al implementar las reglas del sistema, ¿por qué no hacer que los sistemas sean capaces de predefinir los requisitos de privacidad y transparencia en origen?[112]

Además de los esfuerzos llevados a cabo por parte de la Comisionada de Ontario, ya vistos anteriormente, se ha de destacar el esfuerzo del ICO británico que promovió el desarrollo del Privacy Impact Assessment Handbook por Adam Warren de la Universidad de Loughborough[113]. Incluso la Agencia Española de Protección de Datos, publicó una Guía de Evaluación de Impacto en la Protección de Datos Personales[114] indicando

---

[111] El artículo 16 LTBG en relación al acceso parcial establece que «en los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida».

[112] Lessig L. (2001). El código y otras leyes del ciberespacio, Madrid: Taurus y *Lessig L. (2009). Código 2.0. Madrid: Traficantes de sueños*. A idénticas conclusiones llega Guichot Reina. Ver nota a pie de página anterior en la introducción del Capítulo III.

[113] Warren, A.; Bayley, R.; Bennett, C.; Charlesworth, A. J.; Clarke, R.; y Oppenheim, C. (2009). *Privacy Impact Assessments: The UK Experience 31st International Conference of Data Protection and Privacy Commissioners.* Recuperado de https://dspace.lboro.ac.uk/dspace-jspui/bitstream/2134/4481/1/CLSRpaper_revd_280208.pdf

[114]«La Agencia ha decidido elaborar esta *Guía para la Evaluación de Impacto en la Protección de los Datos Personales* con el objeto de promover una cultura proactiva de la privacidad, proporcionando un marco de referencia para el ejercicio de ese compromiso responsable que, a la vez, contribuya a fortalecer la protección eficaz de los derechos de las personas.» Guía para una Evaluación de Impacto en la de Protección Datos Personales. Agencia Española de Protección de Datos - 2014. p. 6. La Guía puede consultarse en http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

que «en la línea de fortalecer la responsabilidad proactiva de quienes tratan datos personales en los sectores público y privado resultan especialmente útiles enfoques como el de la Privacidad desde el Diseño, que propugna que las cuestiones de protección de datos y privacidad se tomen en consideración desde la fase inicial, desde el momento mismo del diseño de un producto o servicio».

3.4.1 Obligación de Evaluación de Impacto en la Protección de Datos

Debemos partir de una premisa básica: el riesgo y la invasión en los derechos se generan por la mera existencia del tratamiento de cierta información personal. Se suele considerar que la tecnología no puede esperar el ritmo del legislador, ya que esto produciría un efecto paralizante para el desarrollo y la innovación. Sin embargo, la Administración, el programador e inventor, o la empresa, desarrollan su tarea en una sociedad determinada regida por unos valores muy concretos.

Con el fin de llevar a cabo las medidas que faciliten la transparencia, cualquier desarrollador debería tener en cuenta una serie de procedimientos en su actuación. El primero de ellos reside en la asunción de los valores positivos inmanentes al desarrollo de actuaciones de diagnóstico previo. Así, el hecho de que cualquiera tenga la capacidad tecnológica de gestar proyectos que proporcionen nuevas prestaciones, e incluso beneficios socialmente relevantes, no le otorga el derecho a hacerlo sin antes verificar su impacto jurídico y social. Ante el desarrollo de una nueva aplicación tecnológica, debe realizarse una evaluación del impacto que esa aplicación pudiera ocasionar en los derechos de los ciudadanos.

En palabras de la propia Agencia Española de Protección de Datos, «entre las herramientas más útiles para avanzar en la privacidad desde el diseño se encuentran las Evaluaciones de Impacto en la Privacidad o en la Protección de Datos, más conocidas como PIAs, por sus siglas en inglés (Privacy Impact Assessments). Una PIA o una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) es, en esencia, un ejercicio de análisis de los riesgos que un determinado sistema de información, producto o servicio puede entrañar para el derecho fundamental a la protección de

datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos. La gran ventaja derivada de la realización de una EIPD en las etapas iniciales del diseño de un nuevo producto, servicio o sistema de información es que permite identificar los posibles riesgos y corregirlos anticipadamente, evitando los costes derivados de descubrirlos a posteriori, cuando el servicio está en funcionamiento o, lo que es peor, cuando la lesión de los derechos se ha producido. Además, la realización de una EIPD es un excelente ejercicio de transparencia, base de una relación de confianza. Ayuda a planificar las respuestas a posibles impactos en la protección de datos de los afectados, a gestionar las relaciones con terceras partes implicadas en el proyecto y a educar y motivar a los empleados para estar alerta sobre posibles problemas o incidentes en relación con el tratamiento de datos personales»[115].

Desgraciadamente, el RGPD no recoge un concepto del término «evaluación de impacto relativa a la protección de datos personales». Sin embargo, sí la encontramos en la normativa relacionada con el sector energético, a propósito de los contadores y las redes inteligentes[116]. De este modo, se trata de un

> *«proceso sistemático para evaluar el impacto potencial de los riesgos cuando las operaciones de tratamiento puedan suponer riesgos específicos para los derechos y libertades de los interesados en razón de su naturaleza, alcance u objetivos, que debe llevar a*

---

[115] Agencia Española de Protección de Datos (2014). Guía para una Evaluación de Impacto en la de Protección Datos Personales, p. 5. Puede consultarse el texto completo en https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

[116] Garriga Domínguez, A. (2016). Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua. Madrid: Dykinson, p. 30. «Los contadores inteligentes son dispositivos electrónicos para medir el consumo de energía en el ámbito doméstico, y que van a permitir la generación, transmisión y análisis de datos sobre los consumidores. El objetivo de los sistemas de contador inteligente y las redes inteligentes es hacer más eficiente y racional la producción, distribución y uso de la energía desde un punto de vista económico y medioambiental, buscando en último término un menor y más racional uso de la misma»

cabo el responsable o el encargado del tratamiento, o el encargado que actúa por cuenta del responsable»[117].

Esta definición es respaldada por el Grupo de Trabajo del Artículo 29[118].

No obstante, sí podemos encontrar una definición del mismo en el documento de trabajo de los servicios de la Comisión europea sobre la evaluación de impacto de la propuesta de RGPD. De este modo, se definiría como un proceso por el cual se hace un esfuerzo consciente y sistemático para evaluar los riesgos a la privacidad de las personas en la obtención, uso y divulgación de sus datos personales. Esta evaluación ayuda a identificar los riesgos para la privacidad, a predecir problemas y a plantear soluciones[119].

El propio RGPD incide en esta aproximación basada en el riesgo, lo que se concreta, en haber introducido[120], la obligación por parte del responsable del

---

[117] Véase al respecto la letra c) del artículo 3 de la RECOMENDACIÓN DE LA COMISIÓN, de 9 de marzo de 2012, relativa a los preparativos para el despliegue de los sistemas de contador inteligente DOUE L73 de 13 de marzo de 2012. Idéntica definición aparece recogida en la letra c) del artículo 2 de la RECOMENDACIÓN DE LA COMISIÓN de 10 de octubre de 2014 relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente. DOUE L 300 de 18 de octubre de 2014.

[118] Así lo reconoce expresamente el Grupo del artículo 29, en el Dictamen 04/2013 sobre el modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente preparado por el Grupo de expertos 2 del Grupo especial sobre redes inteligentes de la Comisión, adoptado el 22 de abril de 2013, WP205. p. 8.

[119] COMMISSION STAFF WORKING PAPER Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC(2012) 72 final, de 25 de enero de 2012. «Data Protection Impact Assessment (DPIA): A process whereby a conscious and systematic effort is made to assess privacy risks to individuals in the collection, use and disclosure of their personal data. DPIAs help identify privacy risks, foresee problems and bring forward solutions».

[120] Me remito al artículo 35.1 RGPD en relación a la Evaluación de impacto relativa a la protección de datos. Así, «cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una

tratamiento de realizar, antes del tratamiento de los datos personales, una evaluación de impacto de las operaciones de tratamiento en la protección de datos personales. Con esta obligación se pretende mejorar el cumplimiento del Reglamento[121], ya que debe servir para que el responsable del tratamiento pueda tomar decisiones por lo que se refiere a «la aplicación de medidas concretas en función del riesgo del tratamiento y de la naturaleza de los datos tratados»[122], y dar así cumplimiento al principio de responsabilidad «accountability». Con esta obligación se espera, incluso, simplificar los procesos de protección de datos para los responsables, asegurando a medio y largo plazo el cumplimiento efectivo de las normas sobre protección de datos personales[123].

---

evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares».

[121] Véase el Considerando 84 RGPD. «A fin de mejorar el cumplimiento del presente Reglamento en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsable del tratamiento la realización de una evaluación de impacto relativa a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relativa a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsable no puede mitigar con medidas adecuadas en términos de tecnología disponible y costes de aplicación, debe consultarse a la autoridad de control antes del tratamiento».

[122] Grupo de trabajo del artículo 29. Dictamen 3/2012 sobre el principio de responsabilidad, de 13 de julio de 2010. GT173. Disponible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_es.pdf

[123] COMMISSION STAFF WORKING PAPER Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC(2012) 72 final, de 25 de enero de 2012. pp 121-122. «DPIAs, however, have the potential to simplify data protection processes for data controllers in the medium- to long-term by ensuring effective compliance with data protection rules. Recent experience in DPIAs in several Member States and internationally has shown that this procedure has beneficial effects in terms of rationalising and streamlining processing operations, and closes potential

En relación a los supuestos que necesitarán el desarrollo de una evaluación de impacto relativa a la protección de datos, aparecen referenciados en el artículo 35.3 RGPD. He de destacar que no nos encontramos ante una lista de actividades o supuestos cerrada. Así, la evaluación se requerirá en particular en los siguientes supuestos:

> *«i) Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; ii) Tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o iii) Observación sistemática a gran escala de una zona de acceso público».*

Será la autoridad de control la encargada de establecer y publicar la lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos. De igual modo, será la misma autoridad de control la que podrá señalar una lista con aquellos tratamientos que no requieran aquella.[124]

Es necesario detenernos en el artículo 35.7 RGPD. En éste, se detalla el contenido mínimo[125] que debe incluir la evaluación de impacto relativa a la protección de datos.

---

gaps in compliance and security. A DPIA can help in identifying and managing data protection risks, avoiding unnecessary costs (in terms of problems being discovered at a later stage), avoiding inadequate dataprocessing solutions, improving the security of personal data and most importantly for an economic operator, avoiding the loss of trust and reputation»

[124] Véase los apartados 4 y 5 del artículo 35 RGPD.

[125] De este modo, «la evaluación deberá incluir como mínimo: a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento; b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad; c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y d) las

3.5 Conclusión

Tener en consideración el derecho a la protección de datos, desde el momento del diseño inicial y del desarrollo de una tecnología, como un elemento más para su buen funcionamiento, responde a una visión de prevención y de reducción de riesgos que puede limitar en gran medida la vulneración de derechos en este contexto.

Tal y como señala la doctrina[126], el derecho es el que debe establecer, en aplicación del principio de precaución, procedimientos que necesiten de una reflexión abierta en la cual deben participar los diferentes actores interesados en el desarrollo de la tecnología.

En consecuencia, los principios de protección de datos desde el diseño y por defecto podrían tener una cierta incidencia en este ámbito, pudiendo resultar herramientas capaces de garantizar la privacidad en un contexto de prevención y de reducción de riesgos.

Cualquier procedimiento de verificación del cumplimiento normativo en materia de privacidad, arroja resultados altamente útiles tanto desde el punto de vista de corregir los riesgos normativos, como en la propia comprensión material de los procesos de captación de información personal y de desarrollo de un modelo de gestión que contemple el ciclo vital de un dato, desde su recogida, hasta su cancelación. No tener en cuenta el impacto de la privacidad, tendría como consecuencia directa bien hacer imposible la satisfacción de los objetivos de transparencia, bien someter al derecho

---

medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas».

126 Poullet, Y. (2011). Internet et Sciences Humaines ou «Comment comprendre l'invisible?». *Revue des Questions Scientifiques*, *182, Issue 4.*, *p. 390*. «C'est au droit à mettre en place, suivant le principe de précaution, des procédures qui obligent à une réflexion ouverte à laquelle doivent prendre part les différents acteurs intéressés au développement de la technologie». El texto complete puede consultarse en el siguiente link: https://www.unamur.be/sciences/philosoc/revueqs/textes-en-ligne/RQS_182_4Internet.pdf

fundamental a la protección de datos a un sacrificio difícilmente justificable. En todo caso, en aplicación del Reglamento resulta necesario realizar por parte de toda organización un análisis o evaluación de los riesgos entes de realizar cualquier tipo de tratamiento, con el fin de determinar qué medidas se aplican y en qué modalidad.

4 EL DERECHO A LA PORTABILIDAD DE LOS DATOS

4.1 Antecedentes.

El RGPD establece un nuevo derecho[127] a favor de los interesados que se configura como un derecho autónomo e independiente a otros derechos reconocidos por la Directiva 95/46/CE.

A finales del año 2007 se creó un grupo de trabajo en Estados Unidos que fue el principal impulsor del desarrollo de este derecho. Se trata del *Data Portability Project*[128]*.* No tardarían en sumarse a este grupo grandes empresas como Google o Facebook en enero de 2008. Pues bien, el *Data Portability Project* estableció como principal objetivo que los usuarios pudieran recuperar el control sobre la información que habían facilitado a un

[127] Expresamente recoge el RGPD en su artículo 20 el Derecho a la portabilidad de los datos en los siguientes términos: «1.El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2.Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3.El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4.El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros».

[128] Para mayor información al respecto, podemos acudir a la siguiente dirección http://www.dataportability.org/

determinado prestador de servicios de la sociedad de la información en el curso de su relación con el mismo.

Con esas premisas, este grupo se propuso adoptar el concepto de la portabilidad de datos como una facultad a favor de los usuarios y una obligación voluntariamente asumida por las empresas que se incluiría entre los términos y condiciones utilizados por los prestadores de servicios de la información a la hora de contratar sus servicios.

El derecho a la portabilidad de los datos ya se incluía en la primera propuesta de RGPD realizada por la Comisión Europea en el año 2012[129]. En ésta, se configuraba este derecho como una facultad del interesado[130]. Con posterioridad, la siguiente versión propuesta de RGPD, publicada tras la primera lectura realizada por el Parlamento Europeo, suprimía por completo el artículo que regulaba este derecho. Se llegó a considerar que el derecho a la portabilidad de los datos no deja de ser una variante del derecho de acceso[131] a los datos personales tratados que no supone grandes

---

[129] La primera versión del RGPD fue publicada el 25 de enero de 2012. Accesible en el link: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

[130] El artículo 18 de la Propuesta reconoce expresamente: «Artículo 18 Derecho a la portabilidad de los datos 1. Cuando se traten datos personales por vía electrónica en un formato estructurado y comúnmente utilizado, el interesado tendrá derecho a obtener del responsable del tratamiento una copia de los datos objeto de tratamiento en un formato electrónico estructurado y comúnmente utilizado que le permita seguir utilizándolos. 2. Cuando el interesado haya facilitado los datos personales y el tratamiento se base en el consentimiento o en un contrato, tendrá derecho a transmitir dichos datos personales y cualquier otra información que haya facilitado y que se conserve en un sistema de tratamiento automatizado a otro sistema en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable del tratamiento de quien se retiren los datos personales».

[131] Véanse las enmiendas 111 y 113 por las que el Parlamento Europeo llegó a «fusionar» ambos derechos, de forma que el derecho a la portabilidad quedaba relegado a una mera vertiente del derecho de acceso. Así se recoge en el Proyecto de Resolución legislativa del Parlamento Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Comisión de Libertades Civiles, Justicia y Asuntos de Interior. El texto completo de la Resolución se encuentra disponible en el siguiente link http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2013-0402+0+DOC+PDF+V0//ES. El texto completo de la Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo

implicaciones ni consecuencias en la operativa de tratamiento de datos personales de los responsables.

Habría que esperar al Planteamiento General del Consejo de la Unión Europea[132] para ver recuperado el derecho a la portabilidad de los datos como derecho autónomo en el texto del RGPD. La versión final de éste recoge principalmente el texto sugerido por el Consejo de la Unión Europea, si bien finalmente se ha optado por sustituir la limitación relativa a la vulneración de «los derechos de propiedad intelectual», por una limitación más genérica. Así, el artículo 20.4 declara expresamente que «el derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros».

Como consecuencia del nuevo entorno digital, aparecen nuevos retos, y los ciudadanos deben seguir teniendo la posibilidad de ejercer un control efectivo sobre su información personal. Es en este contexto en que se incorpora como novedad este derecho. Es cierto que el marco legal impuesto por la Directiva 95/46/CE ya preveía la necesidad de que los responsables del tratamiento pusieran a disposición de los interesados, a solicitud de éstos, una relación de los datos personales que tratan, y que algunas legislaciones nacionales desarrollaron el derecho de acceso determinando los formatos en que la información debía entregarse al interesado[133]. Ahora bien, en esas disposiciones no se concretaba el derecho

---

relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Procedimiento legislativo ordinario: primera lectura) puede encontrarse en el link http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2014-0212+0+DOC+PDF+V0//ES

[132] Planteamiento General del Consejo sobre el Reglamento General de Protección de Datos, de 11 de junio de 2015. Esta versión introduce como novedad una excepción expresa al ejercicio de este derecho. Nos referimos al apartado 2 *bis bis*, al mencionar que «el derecho mencionado en el apartado 2 no se aplicará cuando la revelación de los datos personales vulnere los derechos de propiedad intelectual respecto del tratamiento de dichos datos personales». El texto completo puede consultarse en el siguiente link: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/es/pdf.

[133] Véase al respecto en la normativa española el artículo 15 LOPD y el artículo 28 del RD 1720/2007 que la desarrolla, que establece que «al ejercitar el derecho de acceso, el afectado podrá optar por recibir la información a través de uno o varios de los siguientes sistemas de consulta del fichero: a)

para el interesado, y obligación para el responsable, de entregar los datos tanto al interesado como a un tercer responsable en formatos estructurados, de uso común y lectura mecánica e interoperable.

Afirman FERNÁNDEZ-SAMANIEGO y FERNÁNDEZ-LONGORIA[134] que el nuevo derecho a la portabilidad de los datos sí establece un criterio determinado de formato, que constituye una obligación a cargo del responsable del tratamiento, que no encuentra equivalencia en el derecho de acceso. Además, el ejercicio de este derecho viene supeditado a que se cumplan ciertas condiciones, lo que obligará a los responsables del tratamiento a realizar un análisis previo cuando reciban una solicitud de un interesado que pretende ejercer el derecho a la portabilidad de los datos.

Tal y como estipula el Considerando 68 del RGPD, mediante este muevo derecho se quiere reforzar aún más el control sobre los datos propios en un momento en el que el desarrollo tecnológico ha provocado que los tradicionales derechos de acceso, rectificación, cancelación y oposición no sean suficientes como mecanismo de protección para los titulares de los datos.

4.2 Requisitos del Derecho a la Portabilidad en el RGPD

El derecho a la portabilidad termina de sentenciar que los datos no son propiedad del responsable del tratamiento, sino de la persona a la que hacen referencia, que ahora dispone de un instrumento que le permite recuperarlos «físicamente», superando la típica capacidad de control pasando a un nivel superior, como sería la posesión y movilidad de los datos, ya sea en forma de copia, o como resultado de su transmisión allá donde deseemos. Así,

---

Visualización en pantalla. b) Escrito, copia o fotocopia remitida por correo, certificado o no. c) Telecopia. d) Correo electrónico u otros sistemas de comunicaciones electrónicas. e) Cualquier otro sistema que sea adecuado a la configuración o implantación material del fichero o a la naturaleza del tratamiento, ofrecido por el responsable».

[134] Fernández-Samaniego, J. y Fernández-Longoria, P. (2016). El Derecho a la Portabilidad de los Datos. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus, p. 260.

este derecho persigue «reforzar aún más el control sobre sus propios datos del interesado»[135].

Para ello, a la hora de regular la información que deben facilitar los responsables del tratamiento a los interesados, el RGPD establece la obligación de informar sobre la existencia del derecho a la portabilidad de los datos personales. Así lo hace tanto en el artículo 13[136] relativo a la «información que deberá facilitarse cuando los datos personales se

---

[135] El Considerando 68 del RGPD establece: «Para reforzar aún más el control sobre sus propios datos, cuando el tratamiento de los datos personales se efectúe por medios automatizados, debe permitirse asimismo que los interesados que hubieran facilitado datos personales que les conciernan a un responsable del tratamiento los reciban en un formato estructurado, de uso común, de lectura mecánica e interoperable, y los transmitan a otro responsable del tratamiento. Debe alentarse a los responsables a crear formatos interoperables que permitan la portabilidad de datos. Dicho derecho debe aplicarse cuando el interesado haya facilitado los datos personales dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. No debe aplicarse cuando el tratamiento tiene una base jurídica distinta del consentimiento o el contrato. Por su propia naturaleza, dicho derecho no debe ejercerse en contra de responsables que traten datos personales en el ejercicio de sus funciones públicas. Por lo tanto, no debe aplicarse, cuando el tratamiento de los datos personales sea necesario para cumplir una obligación legal aplicable al responsable o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable. El derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles. Cuando un conjunto de datos personales determinado concierna a más de un interesado, el derecho a recibir tales datos se debe entender sin menoscabo de los derechos y libertades de otros interesados de conformidad con el presente Reglamento. Por otra parte, ese derecho no debe menoscabar el derecho del interesado a obtener la supresión de los datos personales y las limitaciones de ese derecho recogidas en el presente Reglamento, y en particular no debe implicar la supresión de los datos personales concernientes al interesado que este haya facilitado para la ejecución de un contrato, en la medida y durante el tiempo en que los datos personales sean necesarios para la ejecución de dicho contrato. El interesado debe tener derecho a que los datos personales se transmitan directamente de un responsable del tratamiento a otro, cuando sea técnicamente posible».

[136] En concreto nos referimos al apartado 2 b) de este artículo «2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente: …b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el *derecho a la portabilidad de los datos*». Por tanto, los responsables se verán en la obligación de actualizar las cláusulas informativas que utilizan en la recogida de datos, cualquiera que sea el origen de los mismos, para mencionar la posibilidad de ejercer el derecho a la portabilidad de los datos personales.

obtengan del interesado», como en su artículo 14[137] relativo a la «información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado».

El Derecho a la Portabilidad tiene una doble vertiente, y se configura como la facultad que se atribuye al interesado para, en determinadas circunstancias, recibir datos de carácter personal del responsable y por otro lado, poder exigir al responsable que transmita dichos datos a terceros, otro responsable. De esta manera, este derecho cuenta con una doble extensión para el interesado: i) derecho a recibir sus datos en un formato estructurado, de uso común, de lectura mecánica e interoperable; y ii) derecho a exigir al responsable que los transmita a otros responsables del tratamiento[138].

---

[137] En concreto nos referimos al apartado 2 c) de este artículo « 2.Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado: …c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos».

[138] En puridad, esta opción ya se encuentra recogida en nuestra normativa vigente. En concreto, el artículo 22.1 RLOPD prevé que se acuerde de qué manera se llevará a cabo la devolución de los datos, o su transmisión a un tercero, cuando finalice la regulación contractual, todo ello sin disponer de un derecho a la portabilidad. Este artículo, relativo a la conservación de los datos por el encargado del tratamiento, determina que «una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento. No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación». Este es el principal motivo por el que la doctrina se ha preguntado si evitar el riesgo de «lock-in», definido como la situación en la que los datos quedan cautivos de un proveedor se servicio o de un producto informático concreto, de manera que por incompatibilidades de orden técnico no es posible transferir los datos a otro proveedor, o exportarlos a otra aplicación informática, deba formar parte de la regulación de un derecho fundamental, pues se aproxama más a una cuestión contractual o de acuerdos de nivel de servicio, en la relación entre el responsable del tratamiento el encargado del tratamiento. En este sentido se pronuncia, entre otros, Miralles, R. (2013). El derecho a la portabilidad de los datos personales o prestación «premium» del tradicional derecho de acceso. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Pamplona: Aranzadi, p. 288.

Así, los dos condicionamientos de ese derecho son: i) que el tratamiento de los datos personales se efectúe por medios automatizados; y ii) que el interesado hubiera previamente facilitado los datos personales que le conciernan al responsable del tratamiento dando su consentimiento o cuando el tratamiento sea necesario para la ejecución de un contrato. Sin embargo, la opción de recuperar aquello que es nuestro, en un contexto de aplicaciones y servicios electrónicos, no tendría por qué estar vinculada exclusivamente a los datos personales, sino que debería apuntar a cualquier otro tipo de información, incluidos aquellos que han sido generados o calculados a partir de los datos personales obtenidos del interesado.

Asimismo, resulta imprescindible que los responsables colaboren conjunta y proactivamente de manera que los formatos en que se entregan los datos sean «interoperables[139]». Sin embargo, la creación de esos «formatos interoperables» se configura más bien como una recomendación.

Los requisitos que se establecen en el artículo 20 se pueden sintetizar en:

4.2.1.1 Que los datos de carácter personal incumban al solicitante

Cuando los datos conciernan a más de un interesado, el derecho a recibir los datos se entenderá sin menoscabo de los derechos y libertades de los otros interesados. Esta idea aparece reflejada en el artículo 20.4 al indicar que el derecho no afectará negativamente a los derechos y libertades de otros. Aunque no se especifica, se impone al responsable un deber de analizar si el hecho de entregar los datos, puede afectar a los derechos y libertades tanto de otros sujetos a los que se refieren esos datos como a las de otros.

[139] La «interoperabilidad» es definida como la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y conocimiento entre ellos.

4.2.1.2 Que los datos hayan sido facilitados por el interesado al responsable del tratamiento:

Existen multitud de ocasiones en las que tratan datos que no han sido obtenidos directamente del interesado. El derecho a la portabilidad de los datos solo puede hacerse efectivo en aquellos supuestos en los que el interesado hubiese facilitado directamente sus datos al responsable.

4.2.1.3 El tratamiento se base en el consentimiento o en la existencia de un contrato

El artículo 6 del RGPD establece hasta seis condiciones que legitiman la licitud del tratamiento de datos, pero el nuevo derecho a la portabilidad solo resultará de aplicación en dos supuestos:

> *a) Cuando el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b); y b) Cuando el tratamiento se efectúe por medios automatizados.*

Este derecho no puede ejercerse en el resto de los supuestos que legitiman la licitud del tratamiento y, en particular, no puede ejercitarse frente a responsables que traten datos en cumplimiento de obligaciones legales o en cumplimiento de misiones realizadas en interés público o por responsables en el ejercicio de sus funciones públicas.

4.2.1.4 El tratamiento sea automatizado

El ámbito de aplicación material del RGPD se extiende a tratamientos «total o parcialmente automatizados» y también a «tratamientos no automatizados». Sin embargo, al configurarse el derecho a la portabilidad como un derecho a recibir los datos en formato «estructurado, de uso común y lectura mecánica», este derecho se extiende solo a aquellos tratamientos que se efectúen por medios automatizados.

4.3 Contenido del derecho a la portabilidad

Como se ha indicado, el derecho a la portabilidad establece una doble facultad para el interesado. Por un lado, recibir o transmitir datos que le conciernen en un determinado formato y, por otro, a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable que se los hubiera facilitado. Facultad esta última que se complementa con la de poder exigir que el responsable sea el que directamente proporcione los datos a otro responsable cuando sea técnicamente posible. Por tanto, el interesado tiene las siguientes prerrogativas:

1) Entregar datos en formato estructurado, de uso común y lectura mecánica:

   Los requisitos técnicos establecidos en el RGPD no resultan muy precisos. Con ello, el legislador otorga a los responsables del tratamiento una extensa facultad, y no se les impone la forma en la que deben satisfacer el derecho a la portabilidad mediante obligaciones más específicas. Se trata de una obligación de mínimos.

   Sin embargo, se impone que se entreguen en un formato estructurado, sin especificar qué debemos entender por estructurado. El fundamento al que responde este requisito es que los datos se ordenen de una forma estructurada y lógica, con independencia del criterio que se use finalmente, de tal forma que el usuario, o el responsable del tratamiento al que se transmitan los datos, pueda fácilmente identificar y entender qué datos personales está tratando el responsable del fichero una vez que éste le haga entrega de los mismos.

   El Considerando 68 establece que el formato en el que se deben recibir o transmitir los datos debe ser «estructurado, de uso común, de lectura mecánica e interoperable». Sin embargo, esta última característica queda rebajada con posterioridad al aclarar en el propio Considerando que «el derecho del interesado a transmitir o recibir datos personales que lo conciernan no debe obligar al responsable a

adoptar o mantener sistemas de tratamiento que sean técnicamente compatibles» y, por eso, el artículo 20.2 restringe la facultad de que el interesado pueda exigir al responsable que transmita sus datos directamente a otro responsable a aquellos supuestos en que sea «técnicamente posible».

Por último, hacer constar que este artículo 20 no aclara qué sucedería si, en el caso de responsables que utilicen varios sistemas diferentes para el tratamiento de sus datos, estos deberán transformar los datos de un sistema a otro.

Recibir o transmitir los datos y transmisión de responsable a responsable.

El interesado tiene derecho a recibir sus datos y posteriormente enviarlos a otro responsable, pero también tiene derecho a solicitar que sea el responsable el que transmita los datos a otro[140]. En este último supuesto, el interesado se encontrará con una limitación, que no se producía en el primer caso. Y es que mientras que el derecho no se encuentra con ninguna limitación, la transmisión a otro responsable sólo será obligatoria cuando sea técnicamente posible. Así se recalca en el artículo 20.2 RGPD in fine.

Por otra parte, se debe recordar la necesidad de que el traspaso de los datos personales, ya sea de responsable a interesado o de responsable a responsable, no puede realizarse sin observar los deberes que impone el RGPD respecto a la seguridad de los datos. La forma en que se transmita[141] la información deberá garantizar una seguridad adecuada de los datos personales.

---

[140] El artículo 20.2 RGPD dispone expresamente que: «al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible».

[141] No cabe la más mínima duda de que la transmisión, o «comunicación por transmisión» como la recoge el artículo 4.2 RGPD, constituye una modalidad de tratamiento de los datos personales. Como tal tratamiento, se debe de regir por las disposiciones del artículo 5.1 sobre los principios relativos al tratamiento del mismo texto legal. en concreto, la letra f) declara expresamente que los datos personales serán «tratados de tal manera que se garantice una seguridad adecuada de los datos

Como todo derecho, el nuevo derecho a la portabilidad de datos no es absoluto, y el Considerando 73[142] RGPD faculta a que el Derecho de la Unión o de los Estados Miembros pueda imponer restricciones, basadas en criterios de necesidad y proporcionalidad «en la medida en que sea necesario y proporcionado en una sociedad democrática», tales como la salvaguarda de la seguridad pública, la prevención, investigación y enjuiciamiento de infracciones penales y demás objetivos importantes de interés público general de la Unión o de un Estado miembro. El RGPD establece un condicionante para las restricciones, y es que éstas, «han de ajustarse a los dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales». Es en el artículo 23 RGPD donde se recogen y desarrollan estas restricciones. Además, en dicho artículo se determinan las disposiciones específicas que deben contener las medidas legislativas adoptadas por los Estados miembros para poder limitar el alcance del derecho a la portabilidad de los datos.

---

personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)».

[142] El Considerando 73 establece: «El Derecho de la Unión o de los Estados miembros puede imponer restricciones a determinados principios y a los derechos de información, acceso, rectificación o supresión de datos personales, al derecho a la portabilidad de los datos, al derecho de oposición, a las decisiones basadas en la elaboración de perfiles, así como a la comunicación de una violación de la seguridad de los datos personales a un interesado y a determinadas obligaciones conexas de los responsables del tratamiento, en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública o de violaciones de normas deontológicas en las profesiones reguladas, y su prevención, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, la llevanza de registros públicos por razones de interés público general, el tratamiento ulterior de datos personales archivados para ofrecer información específica relacionada con el comportamiento político durante los regímenes de antiguos Estados totalitarios, o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios. Dichas restricciones deben ajustarse a lo dispuesto en la Carta y en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales».

En otro orden de cosas, el artículo 20.3 RGPD establece[143] que el ejercicio del derecho a la portabilidad de los datos se entiende sin perjuicio de la aplicación del denominado derecho de supresión o derecho al olvido. Por tanto, nos encontramos ante dos derechos independientes que los usuarios deberán ejercer de forma separada, de tal forma que salvo que se solicite la supresión de los datos, éstos se podrán seguir tratando por el responsable del tratamiento en el marco de la ejecución de un contrato.

4.4 Portabilidad en el marco del derecho de la competencia

En el actual mercado digital, los datos personales se han convertido en una mercancía de altísimo valor. Las grandes multinacionales tecnológicas dependen cada vez más del tratamiento masivo de datos personales para poder prestar adecuadamente o mejorar sus servicios. Resulta razonable pensar que disponer de gran cantidad de datos personales constituye una ventaja competitiva en el mercado digital y que no tener ningún dato puede ser una barrera de entrada.

En este contexto, las empresas carecen de incentivos para la transmisión de datos a sus competidores, y posiblemente adoptarán estrategias para evitar compartir los datos en la medida de lo posible. Por ello, el derecho a la portabilidad de los datos se ha establecido también con el objetivo de fomentar la competencia en el mercado digital. El propio vicepresidente de la Comisión Europea responsable de la política de la competencia, ALMUNIA, declaró a finales del año 2012 que «en este sentido, creo que uno de los principios de la reforma actual de protección de datos va al corazón de la política de competencia. Como ya he dicho, la propuesta de Reglamento tiene por objeto garantizar el «derecho de la portabilidad». Esto significa que los usuarios deben ser capaces de traspasar sus datos de carácter personal de una compañía a otra sin problemas y costes indebidos.

---

[143] El artículo 20.3 RGPD estipula que «el ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento».

Creo que un ambiente de sana competencia en estos mercados requiere que los consumidores pueden transferir fácilmente y de forma económica sus datos que alojaron en un servicio, a otro servicio. La portabilidad de los datos es importante para aquellos mercados donde la competencia efectiva requiere que los clientes pueden cambiar llevándose sus propios datos con ellos. En aquellos mercados que se basan en los usuarios alojan sus datos personales o su información personal, la retención de estos datos no debe servir como una barrera para el cambio. Los clientes no deben permanecer cautivos en una empresa en particular sólo porque una vez les confiaron sus datos personales».[144]

La portabilidad puede resultar determinante para impedir abusos de posición dominante y facilitar la entrada de competidores en el mercado digital. De hecho, en la misma intervención, el comisario explicó que para facilitar la competencia es posible que la portabilidad de los datos se regule desde un punto de vista del derecho de la competencia.

Con independencia de esas potenciales obligaciones específicas, los mecanismos y recursos generales del derecho a la competencia ya existentes, pueden ser actualmente utilizados para proteger y fomentar la competencia en este mercado. Las autoridades de competencia pueden actuar con base al derecho de competencia en caso de que existan

---

[144] «In this respect, I believe that one of the principles of the current data protection reform goes to the heart of competition policy. As I said, the proposed Regulation aims to ensure the 'right of portability'. This means that users should be able to move their personal data from one company to another without hassle and undue costs. I believe that a healthy competitive environment in these markets requires that consumers can easily and cheaply transfer the data they uploaded in a service onto another service. The portability of data is important for those markets where effective competition requires that customers can switch by taking their own data with them. In those markets that build on users uploading their personal data or their personal content, retention of these data should not serve as barriers to switching. Customers should not be locked in to a particular company just because they once trusted them with their content». La declaración fue realizada el 26 de noviembre de 2012 en el evento «*Privacy Platform Event: Competition and Privacy in Markets of Data*». El texto completo del discurso se encuentra accessible en el siguiente link: http://europa.eu/rapid/press-release_SPEECH-12-860_en.pdf

comportamientos contrarios[145] al mismo en el mercado digital. Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos

4.5 La novedad del principio de transparencia.

A diferencia de la Directiva 95/46/CE[146], el artículo 5 a) del RGPD establece que:

> *«…los datos personales serán tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y trasparencia»)».*

Por tanto, el RGPD contempla un nuevo principio del tratamiento de los datos personales que desarrolla en su artículo 12.

Hemos visto en capítulos anteriores que el tratamiento es lícito cuando tienen apoyo en alguna de las bases legales que lo justifica. En concreto, el RGPD las enumera en su artículo 6[147]. El tratamiento es leal cuando respeta los requisitos, derechos y garantías que la ley establece al efecto.

---

[145] De este modo, el actual artículo 102 (antiguo artículo 82 TCE) del Tratado de funcionamiento de la Unión Europea declara expresamente que «será incompatible con el mercado interior y quedará prohibida, en la medida en que pueda afectar al comercio entre los Estados miembros, la explotación abusiva, por parte de una o más empresas, de una posición dominante en el mercado interior o en una parte sustancial del mismo. Tales prá ticas abusivas podrán consistir, particularmente, en: […] b) limitar la producción, el mercado o el desarrollo técnico en perjuicio de los consumidores».

[146] El artículo 6 a) de la Directiva 95/46/CE dispone que «los datos personales serán tratados de manera leal y lícita».

[147] Véase el artículo 6 RGPD referente a la licitud del tratamiento «1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan

La novedad que supone el principio de transparencia no consiste, pues, en hacer recaer sobre el responsable las obligaciones de informar al interesado acerca de ciertos elementos del tratamiento de sus datos personales, y de comunicarle cómo ha reaccionado al ejercicio de sus derechos. Señala HERNÁNDEZ CORCHETE que, por el contrario, apunta a la manera en que se cumplen dichas obligaciones. El RGPD reconoce que en un entorno tecnológico complejo[148], el mero cumplimiento por el responsable de los indicados deberes no garantiza de un modo efectivo que el interesado sea consciente de la lógica a que obedece el tratamiento de sus datos personales, de modo que crece su percepción de no tener un poder efectivo de disposición sobre ellos, lo que es particularmente grave porque amplios e importantes ámbitos de su actuar se materializan a través de cauces en los que quedan registrados sus datos personales[149]. Esta grave situación es la que se busca solucionar imponiendo que las informaciones indicadas en los artículos 13 y 14 RGPD, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 RGPD, se realicen conforme a un principio de transparencia.

La medida del éxito del nuevo principio vendrá dada por la capacidad de los nuevos modos de comunicación transparente de conferir al usuario la

---

los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones».

[148] En el Considerando 58 del RGPD se afirma expresamente «El principio de transparencia exige que toda información dirigida al público o al interesado sea concisa, fácilmente accesible y fácil de entender, y que se utilice un lenguaje claro y sencillo, y, además, en su caso, se visualice. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. Ello es especialmente pertinente en situaciones en las que la proliferación de agentes y la complejidad tecnológica de la práctica hagan que sea difícil para el interesado saber y comprender si se están recogiendo, por quién y con qué finalidad, datos personales que le conciernen, como es en el caso de la publicidad en línea. Dado que los niños merecen una protección específica, cualquier información y comunicación cuyo tratamiento les afecte debe facilitarse en un lenguaje claro y sencillo que sea fácil de entender».

[149] Hernández Corchete, J. A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus, p 207.

consciencia que ahora le falta acerca del tratamiento de sus datos personales.

4.5.1 La regulación del principio y su génesis

El principio de transparencia aparece configurado en el artículo 12.1 RGPD

> *«El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios».*

La Directiva 95/46/CE no hacía referencia al modo en que el responsable debía suministrar al interesado la información a que estaba obligado. Sin embargo, a la hora de transponerla a nuestro ordenamiento jurídico, la LOPD sí contenía un mandato en este sentido en su artículo 5[150], pues su

---

[150] Afirma el artículo 5 LOPD en relación al derecho de información en la recogida de datos. «1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento. 2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a que se refiere el apartado anterior. 3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban. 4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e

apartado primero disponía que los interesados debían ser informados de modo «expreso, preciso e inequívoco».

Por otro lado, la Resolución de Madrid[151] fijó esta obligación de informar en los apartados 5 y 6 de su artículo 10[152].Por último, el Grupo de Protección de Datos del artículo 29 también se ha preocupado por la forma en la que ha de suministrarse al interesado la información relativa al tratamiento[153]. En este mismo Dictamen del 2011, se advierte expresamente que

---

inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo. 5. No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias. Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten».

[151] Me refiero a la Agencia Española de Protección de Datos. (2009). Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal «Resolución de Madrid»..

[152] El artículo 10 de la «Resolución» de Madrid, dedicado al Principio de Transparencia, declara en sus apartados 5 y 6 «5. Cualquier información que se proporcione al interesado deberá facilitarse de forma inteligible, empleando para ello un lenguaje claro y sencillo, y ello en especial en aquellos tratamientos dirigidos específicamente a menores de edad. 6. Cuando los datos de carácter personal sean recogidos en línea a través de redes de comunicaciones electrónicas, las obligaciones establecidas en el presente apartado podrán satisfacerse mediante la publicación de políticas de privacidad fácilmente accesibles e identificables, que incluyan todos los extremos anteriormente previstos».

[153] Así, reconoce expresamente el Grupo del Artículo 29 que «el consentimiento debe estar «informado». Los artículos 10 y 11 de la Directiva enumeran el tipo de información que debe suministrarse necesariamente a las personas. En cualquier caso, la información suministrada debe ser suficiente para garantizar que los individuos puedan adoptar decisiones bien informadas sobre el tratamiento de sus datos personales. La necesidad de que el consentimiento esté «informado» se traduce en dos requisitos adicionales. En primer lugar, la manera de suministrar información debe garantizar el uso de un lenguaje adecuado que permita al interesado entender lo que está consintiendo y las finalidades. Hay que tener en cuenta el contexto. La utilización de una jerga técnica o jurídica demasiado complicada no cumple los requisitos de la ley. En segundo lugar, la información a los

«La transparencia es una condición para la posesión del control y de validez del consentimiento. La transparencia por sí misma no es suficiente para legitimar el tratamiento de datos personales, pero es una condición esencial para garantizar la validez del consentimiento. Para ser válido, el consentimiento debe estar informado. Esto implica que toda la información necesaria debe suministrarse en el momento en que se solicita el consentimiento, y que éste debe abordar los aspectos sustantivos del tratamiento que el consentimiento se propone legitimar. En principio, debe abarcar las informaciones enumeradas en el artículo 10[154] de la Directiva, pero también depende del momento y las circunstancias en que se solicite el consentimiento. Con independencia de si se otorga o no el consentimiento, la transparencia del tratamiento de datos también es una condición de equidad que sigue siendo válida por si misma incluso después del momento de transmisión inicial de la información».

4.5.2 Libertad de forma

El artículo 12.1 RGPD no impone una forma concreta forma para suministrar al interesado la información. Por tanto, se mantiene la libertad de forma

---

usuarios debería ser clara y suficientemente llamativa para que los usuarios no la puedan pasar por alto. La información debe suministrarse directamente a las personas. No basta con ponerla disposición en algún sitio». Así lo recoge en el Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011. WP187. El texto completo se puede consultar en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf.

154 El artículo 10 de la Directiva 95/46/CE reconoce que «Los Estados miembros dispondrán que el responsable del tratamiento o su representante deberán comunicar a la persona de quien se recaben los datos que le conciernan, por lo menos la información que se enumera a continuación, salvo si la persona ya hubiera sido informada de ello: a) la identidad del responsable del tratamiento y, en su caso, de su representante; b) los fines del tratamiento de que van a ser objeto los datos; c) cualquier otra información tal como: - los destinatarios o las categorías de destinatarios de los datos, - el carácter obligatorio o no de la respuesta y las consecuencias que tendría para la persona interesada una negativa a responder, - la existencia de derechos de acceso y rectificación de los datos que la conciernen, en la medida en que, habida cuenta de las circunstancias específicas en que se obtengan los datos, dicha información suplementaria resulte necesaria para garantizar un tratamiento de datos leal respecto del interesado».

como regla de principio. De igual modo, permite al responsable del tratamiento que tome las medidas oportunas para conseguir el objetivo que el precepto marca como necesario. A éste, por un lado, se le otorga un amplio margen de apreciación sobre cómo ajustar el tratamiento a los requerimientos legales y, por otro, se someten sus decisiones a un control ex post, accountability principle, reconocido en el artículo 24.1 RGPD, y sobre el que tendremos ocasión de profundizar en este mismo capítulo.

Sin embargo, comprobamos cómo se restringe la libertad de forma en la provisión de información al interesado, pues el responsable ha de poder demostrar[155] que el tratamiento se realiza conforme a dicha norma.

4.5.3 La información debe suministrarse directamente, salvo excepciones.

El Grupo del artículo 29 considera que para que realice su función de garantía del consentimiento informado, la información ha de suministrarse directamente a las personas. No basta con ponerla a su disposición en algún sitio[156].

---

[155] Esta obligación de poder demostrar a posteriori el cumplimiento de los requerimientos del RGPD, es una pieza clave y diferencial con respecto al artículo 5 de nuestra LOPD. Además, esa libertad de forma fue la que determinó que la Sentencia del Tribunal Supremo de 15 de julio de 2010 anulara el artículo 18 del RLOPD. De este modo, el Fundamento de Derecho 9 afirma «La Ley reconoce en el artículo 5 el derecho a la información en la recogida de datos, concreta el contenido de la información, y advierte de que el deber de informar ha de ser previo a la recogida, pero salvo la indicación de que la información ha de ser expresa, precisa e inequívoca, ninguna referencia contiene a la forma, abriendo así múltiples posibilidades (escrita, verbal, telemática, etc.) Solo en el apartado 2 del artículo de mención prevé la posibilidad de que se utilicen cuestionarios u otros impresos para la recogida de datos para advertir, pensando sin duda en medios estandarizados, que se han de contener y de forma claramente legible las advertencias expresadas en el apartado 1. En consecuencia, debe considerarse que el legislador ha optado por la libertad de forma. Pues bien, siendo ello así, cabe concluir que la disposición reglamentaria que examinamos contraviene la Ley y que por ello debe ser anulada. Solución distinta se alcanzaría si la letra del precepto impugnado pudiera interpretarse en el sentido de que el medio que previene para cumplir el deber de información se realiza como una mera recomendación, «ad cautelam» de una dificultad probatoria futura, pero los términos categóricos e imperativos utilizados ("deberá llevarse a cabo", "deberá conservar el soporte"), impiden esa valoración. En consecuencia, la impugnación del artículo 18 del Reglamento debe estimarse».

[156] Así lo reconoce el Grupo del Artículo 29 en el Dictamen 15/2011 sobre la definición del consentimiento, de julio de 2011 WP 187, al afirmar expresamente «Para garantizar una información

Por su parte, la Agencia Española de Protección de Datos «ha venido considerando suficiente el cumplimiento del deber de información mediante la existencia de un cartel anunciador siempre que el mismo resulte claramente visible por parte del afectado, quedando así garantizado que el mismo ha podido tener perfecto conocimiento de la información exigible»[157]

4.5.4 Menores

El principio de transparencia rige en particular respecto de cualquier información dirigida específicamente a un niño. Esta precisión normativa insta a considerar la especial posición del niño, caracterizada, más que por una falta de comprensión de la operatividad de un tratamiento, por una limitada conciencia de las consecuencias a largo plazo de determinados comportamientos o incluso, una abierta despreocupación por ellas.

4.5.5 Iconos

En el entorno tecnológico, la información acerca del tratamiento tiende a ser compleja y extensa, lo que supone que el interesado no le preste atención, sea porque no confía en comprenderla, sea porque no quiere *perder* el tiempo que requiere leerla.

---

adecuada se requieren dos tipos de requisitos: i) Calidad de la información - la manera en que se presenta la información (texto claro, sin jerga, comprensible, visible) es esencial para determinar si el consentimiento es manifestación de voluntad «informada». La forma en que se suministra esta información depende del contexto: el usuario medio/habitual debe ser capaz de entenderla; y ii) Accesibilidad y visibilidad de la información – La información debe comunicarse directamente a las personas. No basta con que la información esté «disponible» en algún lugar». La Sentencia del Tribunal de Justicia (Gran Sala) de 5 de octubre de 2004, Pfeiffer Roith, Süß, Winter, Nestvogel, Zeller, Döbele, en los asuntos acumulados C-397/01 a C-403/01, insiste en este punto en relación con un contrato laboral que incluía condiciones no redactadas en el contrato pero mencionadas en él. La información debe ser claramente visible (tipo y tamaño de los caracteres), destacada y completa. Las ventanas de diálogo pueden utilizarse para dar información específica en el momento en que se solicita el consentimiento. Las herramientas de información en línea son especialmente útiles en los servicios de redes sociales para aportar la suficiente precisión y claridad a la configuración de la intimidad. Los avisos breves también puede ser un instrumento útil en este contexto, ya que contribuyen a dar la información correcta de manera fácilmente accesible».

[157] Destacamos los Informes 0304/2005 y 0029/2011.

La norma europea ha buscado que la representación gráfica mediante iconos colabore a una comprensión intuitiva de los caracteres del tratamiento[158]. Sin embargo, tal y como resalta el Grupo del artículo 29, la información mediante iconos por sí sola no es bastante para entender realizado el deber de informar que incumbe al responsable, sirviendo eso sí como complemento de otros medios de informar o, incluso como un recordatorio constante de lo que implica un cierto tratamiento[159].

---

[158] Edwards, L. y Abel, W. (2014). *The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services*. CREATe Working Paper Series. Recuperado de https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf El documento se puede descargar en la siguiente url http://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf

[159] El Grupo del Artículo 29 establece en el Dictamen 16/2011 sobre la recomendación de mejores prácticas de EASA/IAB sobre publicidad comportamental en línea, de 8 de diciembre de 2011. GT188 «En el contexto actual y teniendo en cuenta la actual falta de datos y sensibilización por parte de los usuarios de internet respecto a la publicidad comportamental, la solución del icono no basta por sí misma para informar debidamente a los usuarios sobre el uso de cookies en el sentido del apartado 3 del artículo 5. Esto se debe a las siguientes razones: a) Aunque es posible que en el futuro el icono llegue a ser ampliamente conocido, actualmente el usuario medio no puede reconocer el significado subyacente del icono sin que se explique verbalmente. No obstante, el icono podría resultar útil como complemento de otras formas de aviso informativo, sirviendo de enlace a información adicional sobre los derechos del usuario y de recordatorio constante de que se está siendo objeto de seguimiento; b) Para que la información se presente de forma comprensible, es necesario utilizar un lenguaje claro, que permita a los usuarios comprender inmediatamente que sus actividades están siendo objeto de seguimiento cuando se navega por la red y que, en última instancia, pueden recibir anuncios publicitarios personalizados. El mero uso de la palabra «publicidad» junto al icono no basta para informar al usuario de que el anuncio publicitario utiliza cookies a efectos de publicidad comportamental. El texto debería incluir, como mínimo, la expresión «Publicidad personalizada»; c) El icono pueden servir como información adicional y recordatorio después de que el abonado o usuario haya dado su consentimiento al tratamiento de sus datos para fines de publicidad comportamental. Por consiguiente, la solución del icono que se propone no puede utilizarse para la provisión previa de datos, según lo establecido en el marco jurídico vigente (a menos que se combine con un método para obtener el consentimiento del usuario); y d) La información debe ser correcta y completa, como se establece en el artículo 10 de la Directiva 95/46/CE. El Grupo de Trabajo del artículo 29 desea recordar su dictamen 2/2010, en el que se señala que «Los proveedores de redes de publicidad y los editores deben proporcionar información a los usuarios en cumplimiento del artículo 10 de la Directiva 95/46/CE. En la práctica, deben garantizar que se comunique a los usuarios, como mínimo, quién (es decir, qué entidad) es responsable de instalar el cookie y recoger la información anexa. Además, los usuarios deben estar informados de maneras sencillas de a) que el cookie se utiliza para construir perfiles; b) qué tipo de información se recogerá para construir dichos perfiles; c) que los perfiles se utilizan para suministrar publicidad a medida del usuario y d) que el cookie permite identificar al usuario en múltiples sitios web. Los proveedores y editores de redes deben proporcionar

Este planteamiento es el que se ha llevado a cabo por el artículo 12.7 RGPD, que prevé que

> *«La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente».*

Afirma HERNÁNDEZ CORCHETE[160] que la eficaz realización de la función que se asigna a los iconos depende, de un modo fundamental, de su sencillez (menos información supone mayor claridad), y de que sean universalmente identificables. Este es el motivo por el que el apartado anterior hablaba de *iconos normalizados*, y además, el artículo 12.8 RGPD faculta a la Comisión, de forma indefinida, para adoptar actos delegados, con el fin de especificar la información que se ha de presentar a través de iconos y los procedimientos para proporcionar iconos normalizados.

4.5.6 Certificación

El nuevo marco normativo de protección de datos incentiva la creación de mecanismos de certificación mediante los cuales, el responsable o encargado del tratamiento puedan demostrar el cumplimiento de las obligaciones que legalmente le incumben.

De este modo, el responsable del tratamiento puede acreditar con un sello o marca de protección de datos, que facilita al interesado las

---

información directamente en pantalla, de forma interactiva, si es preciso, mediante mensajes estructurados por niveles. En cualquier caso, la información debe ser accesible y perfectamente visible».

[160] Hernández Corchete, J. A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus, p 213.

informaciones[161] y las comunicaciones tipificadas en el artículo 12 RGPD, e incluso que lo hace de un modo que es acorde con los principios de transparencia vistos anteriormente.

Se ha de tener en cuenta que la certificación no limita la responsabilidad del responsable, no tiene carácter liberatorio. Sin embargo, permitirá que el usuario conozca de un modo sencillo, el nivel de protección de datos de datos de los productos y servicios que considere utilizar, o el tipo de tratamientos que se realiza. Así lo reconoce el Considerando 100[162] del RGPD.

4.6 El deber de suministrar información al interesado (artículos 13 y 14)

4.6.1 Elemento principal del derecho fundamental a la protección de datos

Ya nos hemos referido a las Sentencias del Tribunal Constitucional, 292/2000, de 30 de noviembre, y 29/2013, de 11 de febrero. Por no repetir sus Fundamentos Jurídicos, advertir que en ellas, el Tribunal Constitucional tiene la oportunidad de declarar expresamente que «el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado […] El derecho a la protección de datos garantiza a los individuos un poder de disposición sobre esos datos […]Pero ese poder de disposición sobre los propios datos personales nada vale si el afectado desconoce qué datos son los que se poseen por terceros, quiénes los poseen, y con qué fin».

---

[161] Nos referimos al conjunto de las obligaciones tipificadas en los artículos 13 y 14 del RGPD. Este, hace una distinción atendiendo al origen de la obtención de los datos personales.

[162] El Considerando 100 RGPD declara que «a fin de aumentar la transparencia y el cumplimiento del presente Reglamento, debe fomentarse el establecimiento de mecanismos de certificación y sellos y marcas de protección de datos, que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes».

Pues bien, el poder de disposición que un individuo tiene sobre sus datos personales se manifiesta de modo principal en su capacidad para consentir o rechazar un determinado tratamiento de los mismos, decisión que solo es posible si se le informa previamente de los caracteres definitorios de aquél. De este modo, el deber de informar se conecta de un modo inescindible con el ejercicio de dicho poder de disposición a través del consentimiento. Ahora bien, tal poder de disposición no se agota en ese caso. Cuando un tratamiento de datos personales se apoye en una base jurídica distinta al consentimiento, el titular de los datos mantiene su poder de disposición con una cierta amplitud, pues podrá ejercitar los derechos que en cada caso prevea la legislación aplicable, presupuesto de los cual es que se le haya suministrado información acerca del tratamiento de que se trate y del responsable del mismo[163].

4.6.2 Menciones a las que alcanza el deber de informar, en especial el derecho de portabilidad y la existencia de elaboración de perfiles

Los contenidos sobre los que debe dar cuenta el aviso de privacidad vienen fijados en el RGPD en una enumeración cerrada. Al igual que los artículos 10 y 11 de la Directiva 95/46CE, el artículo 5 LOPD, solo exigía comunicar al interesado informaciones relativas al responsable del tratamiento, a la finalidad de éste, a los destinatarios de la información y a los derechos que asisten al interesado. Si los datos se recogían del interesado, la información debía referirse, además, al carácter obligatorio o no de las respuestas y a las consecuencias derivadas de suministrarlas o de no de hacerlo.

Pues bien, los artículos 13 y 14 RGPD, referidos respectivamente a cada una de estas modalidades de recogida, reproduce la necesidad de que la información contenga los contenidos señalados y, además, añade los siguientes: i) al delegado de protección de datos, en su caso; ii) a la base legal que justifica el tratamiento; iii) al interés legítimo del responsable o de

---

[163] Hernández Corchete, J. A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus, p 214.

un tercero cuando ésta sea la base legal que ampara el tratamiento, y iv) al plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar ese plazo.

La información se proyecta también sobre tres aspectos. De un lado, el responsable debe informar de su intención «de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de éstas o al hecho de que se hayan prestado.»[164]

En segundo lugar, la información sobre los derechos del interesado se amplía en el RGPD respecto de la normativa anterior, ya que, para garantizar un tratamiento de datos leal y transparente, se impone[165] que se refiera expresamente: i) al nuevo derecho a la portabilidad de los datos[166]; ii) al derecho a retirar el consentimiento en cualquier momento en aquellos casos

---

[164] Este deber de información se incluyen en el apartado f) tanto del artículo 13.1 como del artículo 14 del RGPD. Por tanto, da igual de dónde provengan los datos, esta obligación aparece en ambos supuestos.

[165] Al igual que ocurría en la consideración anterior, estos deberes de información se incluyen en el artículo 13.2 como del artículo 14 del RGPD. Por tanto, da igual de dónde provengan los datos, esta obligación aparece en ambos supuestos

[166] Aunque luego me referiré a este nuevo derecho del RGPD, es necesario señalar que el artículo 20 de este texto, se refiere al Derecho a la portabilidad de los datos en los siguientes términos: «1.El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados. 2.Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible. 3.El ejercicio del derecho mencionado en el apartado 1 del presente artículo se entenderá sin perjuicio del artículo 17. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. 4.El derecho mencionado en el apartado 1 no afectará negativamente a los derechos y libertades de otros».

en que la base legal del tratamiento fue éste; y, iii) al derecho a presentar una reclamación ante una autoridad de control.

Por último, se exige comunicar al titular de los datos «la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22[167], apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado[168]».

En este último supuesto encontramos una diferencia notable en relación con lo estipulado en la Directiva 95/46/CE. Así, mientras que el apartado a) del artículo 12 in fine garantiza a todos los interesados el derecho a obtener del responsable del tratamiento «el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el artículo 15.1[169]», en el RGPD la información sobre la lógica utilizada en las decisiones completamente automatizadas debe suministrarla, motu proprio, el responsable del tratamiento en todo caso, y no solo cuando un interesado solicite acceder a los datos que de él tenga el responsable. Ello conlleva por un lado, que dicha información se suministra siempre, y por iniciativa del responsable, y por otro, que se comunica en el estadio más inicial del tratamiento.

---

[167] Véase el artículo 22 RGPD sobre las decisiones individuales automatizadas, incluida la elaboración de perfiles «1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar».

[168] De igual manera, en relación a esta obligación, también da igual de dónde provengan los datos. Así se recoge expresamente en los apartados f) y g) de los artículos 13.2 y 14.2 RGPD, respectivamente.

[169] El artículo 15.1 de la Directiva 95/46/CE relativo a las decisiones individuales automatizadas, expresamente afirma «los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.»

4.6.3 El deber de información cuando el responsable proyecte el tratamiento ulterior de datos personales para un fin distinto (no incompatible)

En los artículos 13 y 14 del RGPD se establece un deber adicional[170] para el responsable del tratamiento al imponer la obligación de informar al interesado cuando proyecte el tratamiento ulterior de los datos para un fin que no sea aquel para el que se recogieron. Esta información se ha de facilitar con anterioridad a dicho tratamiento ulterior, e incluye información sobre la nueva finalidad, y cualquier otra información adicional necesaria.

Recordemos que el artículo 5.1 b) del mismo texto normativo, establece que «los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines»[171].

Entre los fines determinados y explícitos para los que se recogen los datos y los fines que sean incompatibles con aquéllos hay un espacio muy amplio que el RGPD denomina «fin distinto de aquel para el que se recogieron»[172],

---

[170] Me refiero a la exigencia recogida en los apartados 3 y 4 de los artículos RGPD, respectivamente: «Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2».

[171] Idéntica redacción pueden encontrarse en el artículo 6.1 b) de la Directiva 95/46/CE

[172] De este modo se denomina en el artículo 6.4 RGPD «4.Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas: a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto; b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento; c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10; d) las posibles consecuencias para los interesados del tratamiento ulterior previsto; e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización».

o «fin que no sea aquel para el que recogieron»[173], permitiendo que los datos recogidos para un fin puedan ser tratados posteriormente para otro fin que no sea incompatible. Esta configuración aporta flexibilidad al sistema, evitando que el principio de limitación de la finalidad pueda resultar en aplicaciones excesivamente rigoristas. No obstante, y como se ha manifestado, el RGPD prevé algunas garantías desde el punto de vista del interesado. Expresamente me refiero al nuevo deber de información al interesado, que habrá de cumplir el responsable del tratamiento[174].

---

[173] Términos recogidos en los artículos 13 y 14, los cuales he detallado con anterioridad.

[174] A pesar de que haya de realizarse con anterioridad al nuevo tratamiento, la virtualidad de este deber de información no está conectada con el consentimiento del interesado, pues éste no es requisito para que se materialice el ulterior tratamiento. Así se reconoce en el Considerando 50 del RGPD «El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial. En tal caso, no se requiere una base jurídica aparte, distinta de la que permitió la obtención de los datos personales. Si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, los cometidos y los fines para los cuales se debe considerar compatible y lícito el tratamiento ulterior se pueden determinar y especificar de acuerdo con el Derecho de la Unión o de los Estados miembros. Las operaciones de tratamiento ulterior con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos deben considerarse operaciones de tratamiento lícitas compatibles. La base jurídica establecida en el Derecho de la Unión o de los Estados miembros para el tratamiento de datos personales también puede servir de base jurídica para el tratamiento ulterior. Con objeto de determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, el responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento original, debe tener en cuenta, entre otras cosas, cualquier relación entre estos fines y los fines del tratamiento ulterior previsto, el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior, la naturaleza de los datos personales, las consecuencias para los interesados del tratamiento ulterior previsto y la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista. Si el interesado dio su consentimiento o el tratamiento se basa en el Derecho de la Unión o de los Estados miembros que constituye una medida necesaria y proporcionada en una sociedad democrática para salvaguardar, en particular, objetivos importantes de interés público general, el responsable debe estar facultado para el tratamiento ulterior de los datos personales, con independencia de la compatibilidad de los fines. En todo caso, se debe garantizar la aplicación de los principios establecidos por el presente Reglamento y, en particular, la información del interesado sobre esos otros fines y sobre sus derechos, incluido el derecho de oposición […]»

4.6.4 Excepciones

La información al interesado del tratamiento que se haga de sus datos no es un deber absoluto. Hay circunstancias que determinan que el deber de información no nazca[175], y es posible también que, aun existiendo, dicho deber haya de ceder en un caso concreto frente a otros bienes jurídicos prevalentes[176].

Cuando los datos no se han recabado de su titular, el artículo 14.5 RGPD prevé cuatro supuestos en que el deber de información regulado en los apartados 1 a 4 del artículo 14, no surgen. Especialmente me preocupa la reconocida en su apartado b):

> *«…la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de*

---

[175] Los artículos 13.4 y 14.5 del RGPD hacen referencia a esta circunstancia, al indicar el primero de ellos que «las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información». Por su parte, el artículo 14.5 RGPD determina expresamente que «las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que: a) el interesado ya disponga de la información; b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información; c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.»

[176] De este modo se reconoce en el artículo 23.1 RGPD referente a las limitaciones al indicar que «el Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática […]».

investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información».

Y es que, la amplitud[177] de los conceptos o circunstancias que podrían tener cabida en esta excepción hace posible que los distintos aplicadores europeos hagan interpretaciones divergentes, lo que daría al traste con la armonización que el RGPD persigue como objetivo principal.

Lo que sí precisa el artículo 14.5 b) es que esta excepción operará en particular cuando el tratamiento persiga fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, si bien, en estos casos el responsable está sujeto a ciertas garantías que harán que se disponga por su parte las medidas técnicas y organizativas necesarias para garantizar el respeto del principio de minimización de los datos personales. Esta obligación, recogida en el artículo 89.1[178] RGPD, puede incluir la

---

[177] Al igual que la Directiva 95/46/CE en su artículo 11, el articulado del RGPD no recoge criterio alguno para comprobar si la petición de información es realmente desproporcionada. Sin embargo, el artículo 5.5 de la LOPD, sí especifica y señala los criterios tendentes a considerar si la petición es desproporcionada. De esta forma, «no será de aplicación lo dispuesto en el apartado anterior, […] cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias». Sin embargo, estos parámetros aparecen recogidos en el Considerando 62 del RGPD in fine en los siguientes términos «no es necesario imponer la obligación de proporcionar información […] cuando facilitar la información al interesado resulte imposible o exija un esfuerzo desproporcionado. Tal podría ser particularmente el caso cuando el tratamiento se realice con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos. A este respecto, debe tomarse en consideración el número de interesados, la antigüedad de los datos y las garantías adecuadas adoptadas».

[178] El artículo 89.1 RGPD está dedicado a las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos**:** «el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o

seudonimización de los datos, siempre que de esa forma puedan alcanzarse dichos fines.

Esta previsión aporta un importante grado de flexibilidad a los tratamientos que persigan estos fines, restando algo de virtualidad a los derechos de los titulares de los datos. Sería posible que datos, recabados inicialmente con una cierta finalidad de una fuente distinta a su titular, fueran ulteriormente tratados con fines de archivo en interés público, de investigación científica o histórica o de estadística, tratamiento ulterior del que el responsable no estaría obligado a informar al interesado. El resultado es que el interesado habrá sido informado de que sus datos están siendo tratados con una determinada finalidad cuando en realidad, en virtud de un segundo tratamiento del que no ha sido informado, están siendo tratados con fines de archivo en interés público, de investigación científica o histórica o de estadística.

Este apartado b) del artículo 14.5 RGPD también exceptúa el deber de información cuando cumplirlo «pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento». Con esta excepción, lo que se está protegiendo es la posición jurídica individual o colectiva a que sirve el tratamiento.

4.7 El Derecho de acceso del interesado (art. 15)

Afirma TRONCOSO REIGADA que desde la Sentencia del Tribunal Constitucional 254/1993, de 20 de julio de 1993, se viene considerando que el derecho de acceso del interesado es un aspecto central del derecho del

---

fines estadísticos estará sujeto a las garantías adecuadas, con arreglo al presente Reglamento, para los derechos y las libertades de los interesados. Dichas garantías harán que se disponga de medidas técnicas y organizativas, en particular para garantizar el respeto del principio de minimización de los datos personales. Tales medidas podrán incluir la seudonimización, siempre que de esa forma puedan alcanzarse dichos fines. Siempre que esos fines pueden alcanzarse mediante un tratamiento ulterior que no permita o ya no permita la identificación de los interesados, esos fines se alcanzarán de ese modo».

interesado a la protección de sus datos personales[179]. Se ha comentado anteriormente que el artículo 8.2. de la Carta de los Derechos Fundamentales de la Unión Europea[180] prevé expresamente que nos encontramos ante una facultad integrante del mismo.

Es esta función instrumental, reconocida por el Tribunal de Justicia de la Unión Europea[181]. Solo conociendo los datos personales que un responsable tiene de ella, una persona está en condiciones de comprobar que el tratamiento cumple las exigencias legales y de ejercitar los derechos regulados en los artículos 16 a 22 RGPD.

El artículo 15 RGPD[182] extiende la información a la que cabe acceder respecto de la prevista en el artículo 12 de la Directiva 95/46/CE y artículo

---

[179] Véase al respecto Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant Lo Blanch, pp. 111 y ss. El texto de la STC 254/1993, de 20 de julio de 1993, se encuentra accesible en https://www.boe.es/boe/dias/1993/08/18/pdfs/T00028-00034.pdf.

[180] El artículo 8.2 de la Carta de los Derechos Fundamentales de la Unión Europea (DOCE C364 de 18.12.2000) afirma que «estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación». Texto accesible en el link http://www.europarl.europa.eu/charter/pdf/text_es.pdf.

[181] Los §51 y §52 de la Sentencia del Tribunal de Justicia de 7 de mayo de 2009, College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer, asunto C-553/07, afirman que «El citado derecho de acceso es indispensable para que el interesado pueda ejercer los derechos que se contemplan en el artículo 12, letras b) y c), de la Directiva, a saber, en su caso, cuando el tratamiento no se ajuste a las disposiciones de la misma, obtener del responsable del tratamiento de los datos, la rectificación, la supresión o el bloqueo de los datos [letra b)], o que proceda a notificar a los terceros a quienes se hayan comunicado los datos, toda rectificación, supresión o bloqueo efectuado, si no resulta imposible o supone un esfuerzo desproporcionado [letra c)]. El derecho de acceso es, igualmente, condición necesaria para el ejercicio por el interesado del derecho de oposición al tratamiento de sus datos personales, contemplado en el artículo 14 de la Directiva, como lo es para el derecho a recurrir por los daños sufridos, previsto en los artículos 22 y 23 de ésta». http://curia.europa.eu/juris/document/document.jsf?text=&docid=74028&pageIndex=0&doclang=es&mode=lst&dir=&occ=first&part=1&cid=157824

[182] El Derecho de acceso es regulado en el artículo 15 RGPD en los siguientes términos «1.El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información: a) los fines del tratamiento; b) las categorías de datos personales de que se trate; c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales; d) de ser posible, el plazo previsto de conservación de los datos

15 LOPD, comprendiendo los mismos contenidos a que alcanza el deber de información ex artículos 13 y 14.

El artículo 15 RGPD especifica que el interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en ese supuesto, obtener el «derecho de acceso a los datos personales y a la siguiente información […]», con lo que enfatiza que el acceso se proyecta también sobre la información relativa al tratamiento, que en sentido estricto no son datos personales[183] del

personales o, de no ser posible, los criterios utilizados para determinar este plazo; e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento; f) el derecho a presentar una reclamación ante una autoridad de control; g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen; h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado. 2.Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia. 3.El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común. 4.El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros».

[183] La misma Sentencia del Tribunal de Justicia de 7 de mayo de 2009, asunto C-553/07 distingue en los § 42 y §43 dos tipos de datos que pueden entrar en juego. «El primer tipo se refiere a los datos de carácter privado sobre una persona, que obran en poder del municipio, como el nombre o domicilio, que constituyen, en este caso, los datos principales. Se desprende de las observaciones orales formuladas por el College y el Gobierno neerlandés, que tales datos pueden ser objeto de un plazo de conservación más largo. Constituyen «datos personales» en el sentido del artículo 2, letra a), de la Directiva, puesto que se trata de información sobre una persona física identificada o identificable (véanse, en este sentido, las sentencias de 20 mayo de 2003, Österreichischer Rundfunk y otros, C‑465/00, C‑138/01 y C‑139/01, Rec. p. I‑4989, apartado 64, de 6 noviembre de 2003, Lindqvist, C‑101/01, Rec. p. I‑12971, apartado 24, y de 16 de diciembre de 2008, Huber, C‑524/06, Rec. p. I‑0000, apartado 43). […] El segundo tipo atañe a la información sobre los destinatarios o categorías de destinatarios a quienes se comunican los datos principales y a la información sobre el contenido de éstos, por lo que hace referencia al tratamiento de los datos principales. Conforme a la normativa nacional controvertida en el procedimiento principal, la conservación de dicha información se limita al período de un año».

interesado, pudiendo aludir incluso a otras personas como, por ejemplo, los destinatarios de la cesión de esos datos.

En relación a la forma, el artículo 15.3, tan solo afirma que «el responsable del tratamiento facilitará una copia de los datos personales, objeto de tratamiento…Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común».

La función instrumental de este derecho ha sido tenida en cuenta por el Tribunal de Justicia de la Unión Europea[184] para sentar que ha de materializarse en un modo que permita al interesado verificar que el tratamiento cumple con la ley y, en su caso, ejercer los derechos que los artículos 16 a 22 le otorgan.

Este derecho tampoco es absoluto. El artículo 23.1 RGPD permite que «el Derecho de la Unión o de los Estados miembros que se aplique al responsable o el encargado del tratamiento podrá limitar, a través de medidas legislativas, el alcance de las obligaciones y de los derechos establecidos en los artículos 12 a 22 y el artículo 34, así como en el artículo 5 en la medida en que sus disposiciones se correspondan con los derechos y obligaciones contemplados en los artículos 12 a 22, cuando tal limitación respete en lo esencial los derechos y libertades fundamentales y sea una medida necesaria y proporcionada en una sociedad democrática para salvaguarda» de alguno de los fines que enuncia.

---

[184] La Sentencia del Tribunal de Justicia de 12 de diciembre de 2013, petición de decisión prejudicial planteada por el Gerechtshof te ´s-Hertogenbosch, asunto C-486/12, expresamente declara en su Fallo: « 1) El artículo 12, letra a), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que no se opone a la percepción de gastos por la comunicación de datos de carácter personal por una autoridad pública. 2) El artículo 12, letra a), de la Directiva 95/46 debe interpretarse en el sentido de que, para garantizar que los gastos percibidos con ocasión del ejercicio del derecho de acceso a los datos de carácter personal no sean excesivos a efectos de esa disposición, el importe de esos gastos no debe exceder el coste de la comunicación de dichos datos. Incumbe al tribunal remitente llevar a cabo las verificaciones necesarias en relación con las circunstancias del litigio principal».

Por otro lado, ya se ha indicado que los apartados 2 y 3 del artículo 89 RGPD hacen lo propio respecto de los tratamientos que persigan fines de archivo en interés público, e investigación científica o histórica o de estadística. Así como, el artículo 15.4 RGPD prevé una restricción consistente en que el ejercicio de este derecho «no afectará negativamente a los derechos y libertades de otros».

Todos estos supuestos tienen en común que el derecho de acceso del interesado colisiona con derechos o intereses de terceros u otros bienes jurídicos que, mereciendo también protección, determinan que aquél sea limitado o incluso excepcionado por completo. Su aplicación no es automática, sino que implica siempre una ponderación de unas y otras situaciones jurídicas en la que es esencial evaluar la necesidad de la restricción para el fin perseguido y, en tal caso, la proporcionalidad del sacrificio.

4.8 Conclusiones

Es cada vez más evidente que la información es esencial en la vida de las personas y para la marcha de la economía. El RGPD persigue establecer un régimen único, muy especialmente en lo que hace a las garantías de que los datos personales de los individuos estarán adecuadamente protegidos, que aparecen reforzadas, de un lado, mediante la ampliación de los elementos del tratamiento que abarca el deber de información y el derecho de acceso y, de otro, exigiendo que el modo en que el responsable cumpla estas obligaciones sea transparente, esto es, comprensible para el interesado, todo ello con la finalidad de que aumente la conciencia de este último sobre el control que tienen de sus datos personales.

5 LA NOTIFICACIÓN DE LAS VIOLACIONES DE SEGURIDAD

5.1 Introducción y conceptos sobre seguridad de los datos y violaciones de seguridad

5.1.1 Postulados básicos de la política de seguridad de los datos

Antes de entrar en el contenido del epígrafe, y referirme a las violaciones de seguridad, me gustaría hacer referencia a los considerados postulados básicos sobre los que ha de asentarse la política de seguridad de los datos, partiendo del concepto de responsabilidad sobre el tratamiento de los mismos. Estos planteamientos se concretan en los siguientes principios:

a) Se debe establecer la responsabilidad general del responsable por cualquier tratamiento de datos personales realizado por él mismo o en su nombre, con el fin de asegurar la accountability o rendición de cuentas. En particular, el responsable del tratamiento debe garantizar y está obligado a demostrar que cada operación de tratamiento cumple lo dispuesto en el RGPD.
b) La protección de los derechos y libertades de los interesados con respecto al tratamiento de datos personales exige la adopción de las oportunas medidas de carácter técnico y organizativo, tanto en el momento del diseño del tratamiento como en la realización del mismo, con el fin de garantizar que se cumpla lo dispuesto en el RGPD. Para ello, el responsable debe adoptar las políticas internas y aplicar las medidas adecuadas que cumplan especialmente con los principios de protección de datos desde el diseño y por defecto.

Afirma PUYOL MONTERO[185], y así he intentado reflejarlo a lo largo de este trabajo, que el principio de protección de datos desde el diseño requiere la integración de la protección de datos en todo el ciclo de vida de la tecnología, desde la primera fase de diseño hasta su despliegue, su utilización y, finalmente, en lo que atañe a su eliminación definitiva. Por su parte, el principio de protección de datos por defecto exige que la configuración de la privacidad de los servicios y productos cumpla por defecto los principios generales de la protección de datos, como la minimización de los datos y la limitación de los fines.

Expone CARPIO CÁMARA[186] que el responsable y el encargado debe entender la seguridad del tratamiento como un proceso y no como un hito de cumplimiento. Deben demostrar una responsabilidad proactiva en el cumplimiento de los principios de protección de datos de forma que se pueda acreditar, accountability, este proceso continuo. Ello redundará no solo en interés de los titulares de los datos, sino también en la mejora de la productividad, la reputación de la empresa y la implicación de los trabajadores.

c) Para demostrar la conformidad con el RGPD, el responsable o el encargado del tratamiento deben documentar cada operación de tratamiento, con el fin de ser capaces de facilitar suficiente información a los interesados. Todos los responsables y encargados del tratamiento están obligados a cooperar con la autoridad de control y a poner a su disposición, previa solicitud, como mínimo dicha información, de modo que pueda servir para supervisar las operaciones de tratamiento.

---

[185] Puyol Montero, J. (2015). La regulación de las medidas de seguridad. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo derecho europeo de protección de datos: Towards a new european data protection regime*. Valencia: Tirant lo Blanch, pp 669-702

[186] Carpio Cámara, M. (2016). Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Editorial REUS, pp 347-348.

d) Uno de los aspectos principales es definir con precisión las actuaciones denominadas brechas de seguridad, incidentes de seguridad, violaciones de datos, etc.

Todas ellas se enmarcan en una materia que progresivamente ha cogido relevancia en las organizaciones para la protección de sus activos intangibles: la seguridad de la información. Esta, tiene reconocida tres dimensiones diferentes y complementarias: i) La confidencialidad. Es decir, que solo acceda a la información quien debe conocerla; ii) La integridad. Es decir, que la información no pueda ser manipulada o alterada, y por lo tanto, que no pierda su carácter informador; y, iii) La disponibilidad. Es decir que esté accesible en el momento que se necesita.

Existen muy diversas amenazas que, aprovechando una vulnerabilidad, provocan un impacto en la seguridad de la información. La operadora de comunicaciones estadounidense Verizon publica anualmente un informe titulado “Data Breach Investigations Report”. El último report187 accesible es de este mismo año 2017, y destaca que se hayan producido más de cien mil incidentes de seguridad. De ellos, 1.935 son data breaches confirmados188. Pero en realidad, ¿qué entendemos por data breach? Pues bien, existen diferentes tipologías de actos que podrían considerarse “violaciones de datos” o “brechas de seguridad”, tales como: i) Ataques telemáticos desde el exterior de una red corporativa; ii) Utilización de ingeniería social para hacerse con claves de usuarios autorizados, el intruso puede realizar diversas acciones cuando esté

---

[187] El texto del informe se encuentra disponible en el siguiente link http://www.verizonenterprise.com/resources/reports/rp_DBIR_2017_Report_en_xg.pdf

[188] El mismo informe nos resalta la terminología empleada: i) Incident: A security event that compromises the integrity, confidentiality or availability of an information asset; ii) Breach: An incident that results in the confirmed disclosure (not just potential exposure) of data to an unauthorized party. A nivel interno, una definición del término «incidencia» nos la ofrece la letra i) del 5.2 del RLOPD, en los siguientes términos «cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos».

dentro del sistema, ya sea, apropiarse de información confidencial y difundirla posteriormente o venderla, encriptarla y solicitar un "rescate", o simplemente destruir la información sin sacarla de la red corporativa, etc.; iii) Mal uso de información realizada por un usuario trabajador de una red corporativa, teniendo acceso legítimo ese sistema en base a su labor; o, iv) Ataque desde dentro de un trabajador intentando acceder a información a la que no debería.

e) Con objeto de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el RGPD, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos.

   El RGPD requiere que los responsables y encargados del tratamiento asuman el papel de proteger la privacidad de los afectados más allá de la implementación de una serie de medidas de seguridad concretas. Serán, ellos quienes deban evaluar el riesgo que supone para la privacidad de los afectados el tratamiento de datos que realizan.

   El RGPD introduce un enfoque basado principalmente en el riesgo, de modo que las medidas técnicas y organizativas de seguridad deben venir determinadas y justificadas, mediante la realización de una previa evaluación de los mismos que debe incluir, las medidas, garantías y mecanismos previstos para garantizar la protección de los datos personales y demostrar la conformidad con el RGPD. Éste, no establece un listado de las medidas de seguridad que son de aplicación de acuerdo con la tipología de datos objeto de tratamiento, sino que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas adecuadas al riesgo que conlleva el tratamiento. Esto supone un importante cambio, en el que se modifica la obligatoriedad de implementar un catálogo de medidas de seguridad concretas, por la responsabilidad de evaluar el riesgo que entraña para la privacidad y tratamiento de datos, así como la implementación de las medidas de seguridad apropiadas para mitigar

estos riesgos introduciendo así, la variable de los costes de las medidas de seguridad.

Esta evaluación de riesgo puede conllevar a una mayor conciencia de los citados responsables y encargados, sobre la necesidad de ceñirse los tratamientos de datos estrictamente necesarios, lo que podría impulsar la utilización de tecnologías que minimicen los riesgos de privacidad, mediante el empleo de nuevas técnicas que propicien la seudonimización o anonimización de la información, aumentando de este modo, y de manera muy notable, las garantías de protección de la información personal de los ciudadanos.

Por ello, la determinación de controles, en respuesta a los riesgos identificados, deberá tener en cuenta las técnicas existentes y los costes de implementación, lo que establece una clara decisión por la gestión de la privacidad basada en los riesgos. Estas medidas deben garantizar un nivel de seguridad adecuado, teniendo en cuenta el estado de la técnica y el coste de su aplicación, en relación con los riesgos y la naturaleza de los datos que deban protegerse. El análisis de una organización desde el punto de vista del riesgo se basa en identificar vulnerabilidades una por una y fijar cada una de ellas, y variará en función de los tipos de tratamiento, de la naturaleza de los datos que se traten, del número de interesados afectados o de la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

f) Una violación de los datos personales puede causar, si no se toman medidas de manera rápida y adecuada, pérdidas económicas sustanciales y perjuicios sociales muy relevantes al responsable del tratamiento que tenga conocimiento de que se ha producido una violación de seguridad. Las personas cuyos datos personales puedan verse afectados negativamente por tal brecha de seguridad deben ser informadas de ello sin demora injustificada para que puedan adoptar las cautelas necesarias.

Se debe considerar que una violación afecta negativamente a los datos personales o la intimidad de los interesados, cuando conlleva, por ejemplo, fraude o usurpación de identidad, daños físicos, humillación grave o perjuicio para su reputación. La notificación debe describir la naturaleza de la violación de los datos personales y las recomendaciones para que la persona afectada mitigue sus potenciales efectos adversos.

g) El RGPD declara como interés legítimo del responsable del tratamiento el garantizar la seguridad de la red y de la información, es decir la capacidad de una red o de un sistema de información de resistir, en un nivel determinado de confianza, a acontecimientos accidentales o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos personales conservados o transmitidos, y la seguridad de los servicios conexos ofrecidos por, o accesibles a través de, estos sistemas y redes, por parte de autoridades públicas, equipos de respuesta a emergencias informáticas, equipos de respuesta a incidentes de seguridad informática, proveedores de redes y servicios de comunicaciones electrónicas y proveedores de tecnologías y servicios de seguridad. En lo anterior cabría incluir, por ejemplo, impedir el acceso no autorizado a las redes de comunicaciones electrónicas y la distribución malintencionada de códigos, y frenar ataques de «denegación de servicio» y daños a los sistemas informáticos y de comunicaciones electrónicas.
h) A diferencia de los que ocurre con el RLOPD, que en su Título VIII contiene un catálogo detallado de las medidas que las empresas deben adoptar en función de la naturaleza de los datos, ya sean medidas de nivel básico, medio o, alto, el RGPD no establece ningún catálogo de controles. Aunque se deja al arbitrio del responsable y del encargado la selección de medidas apropiadas para garantizar el nivel de protección adecuado al riesgo, a lo largo del RGPD se trata de persuadir a ambos roles de que lo más eficiente será su adhesión a un futuro código de conducta que encaje con el tipo de organización

y tratamiento. Aparentemente se persigue una corregulación, pues serán las asociaciones y otros organismos representativos de los responsables y encargados los que redacten los códigos de conducta y, posteriormente la Autoridad de Control y, en su caso, el Comité Europeo de Protección de Datos, quienes los aprobarán.

Sin descender a mayores detalles, el RGPD exige que los códigos de conducta incluyan medidas que garanticen la confidencialidad, integridad, disponibilidad y resiliencia[189] permanentes en los sistemas y servicios de tratamiento, la capacidad de restaurar la disponibilidad y el acceso a los datos en caso de incidente físico o técnico, además de un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas de seguridad.

Sorprendentemente, el RGPD se decide a concretar en una medida en particular al sugerir repetidamente mecanismos de cifrado y seudonimización para garantizar la confidencialidad de ciertos tratamientos. Los futuros códigos de conducta deberán discriminar en qué tratamientos y con qué categorías de datos resultará suficiente una seudonimización, una anonimización o, en último término, deberán cifrarse los datos.

---

[189] Una definición de este concepto la encontramos en Salvador Carrasco, L. (2015). Ciber-resiliencia. *Boletín electrónico del Instituto Español de Estudios Estratégicos*, *35*, pp. 3-4. «Resiliencia se define como una cualidad intrínseca, una característica propia de una organización que le permite enfrentarse de forma exitosa a los cambios y a los eventos tanto internos como externos. La resiliencia forma parte de la naturaleza de dicho organismo y está implícita en su estructura. Cuando una entidad se etiqueta como resiliente es porque se observa que, ante una serie de sucesos, la organización ha sabido reaccionar y externamente continúa operando como si nada hubiera ocurrido. Por lo tanto, el término resiliente se puede aplicar tanto a una empresa como a un sector económico, a un gobierno, a un estado nacional o incluso un organismo vivo, a estructuras sociales como mercados, a comunidades o ejércitos. […] La gestión del cambio forma parte de la resiliencia de una organización. Una entidad será resiliente cuando se enfrente de forma exitosa tanto a los cambios que se desarrollan de forma progresiva, como a los que se desaten de forma violenta». Recuperado de http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO35-2015_Ciber-resiliencia_LuisdeSalvador.pdf

5.2 Marco normativo relacionado con las violaciones de seguridad

5.2.1 La normativa de protección de datos: desde la Directiva 95/46/CE pasando por la LOPD y el RLOPD

La Directiva 95/46/CE establecía la obligación general de notificar el tratamiento de datos personales a las autoridades de control. Éstas realizarían las comprobaciones previas sobre los posibles riesgos para los derechos y libertades de los interesados una vez que haya recibido la notificación. Pues bien, a pesar de que esta obligación implica cargas administrativas y financieras, no contribuyó, sin embargo, en todos los casos a mejorar la protección de los datos personales.

Actualmente, la vigente LOPD no establece una obligación de comunicar violaciones de datos, brechas de seguridad o incidentes similares a una Autoridad de Control. Sin embargo, sí regula la necesidad de implantar la seguridad adecuada en los ficheros con datos personales a través de su artículo 9, que insta a responsables de ficheros y encargados del tratamiento a «adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural».

Se trata de una obligación genérica del deber de custodia de la información para garantizar su seguridad. No obstante, la realidad nos demuestra que la seguridad plena no existe, pero, además, el coste de garantizar la seguridad de los datos al 100% tendría un coste ilimitado. Sería inalcanzable para cualquier entidad.

Este principio de seguridad de los datos es desarrollado por el RLOPD, que, si bien no regula tampoco un régimen de notificación de violaciones de datos a una Autoridad de Control, sí recoge algunas obligaciones en torno a dos medidas de seguridad relacionadas con dicho fenómeno, como son: i) el

registro de incidencias[190]; y, ii) los procedimientos de recuperación de datos[191].

Por todo ello, comprobamos que existe un deber genérico de protección de datos en la LOPD y dos tipos de medidas concretas, la gestión de incidencias y los procedimientos de recuperación, que hacen referencia a obligaciones y procedimientos que debe implementar la entidad que "sufre" una pérdida o destrucción de datos, o en general cualquier anomalía que afecte a la seguridad de sus dicheros con datos personales.

5.2.2 Ley General de Telecomunicaciones

Para entender e interpretar correctamente las obligaciones establecidas en la LGTel[192], es fundamental conocer el significado de "violació de los datos personales". Esta definición nos la ofrece el artículo 41 de la LGTel.

> *«A los efectos establecidos en este artículo, se entenderá como violación de los datos personales la violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con*

---

[190] En este sentido, conforme al artículo 90 RLOPD, las compañías que traten datos en ficheros calificados de nivel básico, deben tener «un procedimiento de notificación y gestión de las incidencias que afecten a los datos de carácter personal y establecer un registro en el que se haga constar el tipo de incidencia, el momento en que se ha producido, o en su caso, detectado, la persona que realiza la notificación, a quién se le comunica, los efectos que se hubieran derivado de la misma y las medidas correctoras aplicadas». Si los datos pertenecen a un fichero de nivel medio, además de lo indicado anteriormente, también deberán consignarse «los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación», tal y como dispone el apartado primero del artículo 100 del mismo texto legal anteriormente señalado.

[191] El artículo 94.2 RLOPD dispone que «se establecerán procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Únicamente, en el caso de que la pérdida o destrucción afectase a ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación permita alcanzar el objetivo al que se refiere el párrafo anterior, se deberá proceder a grabar manualmente los datos quedando constancia motivada de este hecho en el documento de seguridad».

[192] Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, BOE núm 114, de 10/05/2014

la prestación de un servicio de comunicaciones electrónicas de acceso público».

Coincido con SÁIZ PEÑA al advertir que se trata de un concepto muy amplio, donde no se establece ningún tipo de métrica cualitativa ni cuantitativa, por lo que se podría entender que un operador está obligado a notificar una violación de datos, tanto si su base de miles de clientes ha sido hackeada, como si por una negligencia por parte de un trabajador se han alterado datos de cinco clientes en los sistemas[193].

Pues bien, el artículo 41.2 de la LGTel establece que «en caso de que exista un riesgo particular de violación de la seguridad de la red pública o del servicio de comunicaciones electrónicas, el operador que explote dicha red o preste el servicio de comunicaciones electrónicas informará a los abonados sobre dicho riesgo y sobre las medidas a adoptar».

Es en el artículo 41.3 LGTel donde se reconoce la competencia de la Agencia Española de Protección de Datos como Autoridad a la que notificar las violaciones de datos personales por parte del operador de servicios de comunicaciones electrónicas disponibles al público «sin dilaciones indebidas». Asimismo, «si la violación de los datos pudiera afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el operador notificará también la violación al abonado o particular sin dilaciones indebidas».

No obstante, esta obligación de notificación a un abonado o al particular afectado, no será necesaria «si el proveedor ha probado a satisfacción de la Agencia Española de Protección de Datos que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad». Sin embargo, y a pesar de la obligación de informar los abonados o particulares, en el supuesto de que el proveedor no les hubiera notificado ya, «la Agencia Española de

---

[193] Sáiz Peña, C. A. (2015). La notificación de brechas de seguridad. En Rallo Lombarte A; García Mahamut, R. (dir.): *Hacia un nuevo derecho europeo de protección de datos.* Valencia: Tirant lo Blanch, p. 780.

Protección de Datos podrá exigirle que lo haga, una vez evaluados los posibles efectos adversos de la violación».

Este artículo continúa regulando el contenido de dichas notificaciones de violaciones de datos, diferenciado éste en relación al destinatario del mismo. Si la notificación va dirigida al abonado o al particular, «se describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información y se recomendarán medidas para atenuar los posibles efectos adversos de dicha violación». En el supuesto de que la notificación vaya dirigida a la Agencia Española de Protección de Datos, «se describirán además las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales».

Adicionalmente, se obliga a los operadores a realizar un inventario «de las violaciones de los datos personales, incluidos los hechos relacionados con tales infracciones, sus efectos y las medidas adoptadas al respecto, que resulte suficiente para permitir a la Agencia Española de Protección de Datos verificar el cumplimiento de las obligaciones de notificación reguladas en este apartado».

La LGTel también regula unas obligaciones similares, relacionadas con la notificación de violaciones de seguridad o pérdida de integridad, sin vincularlo a los datos personales. En concreto, estas obligaciones de notificación se regulan en su artículo 44[194], referente a la «integridad y

[194] Véase el artículo 44 LGTel en el que expresamente se determina que «1. Los operadores de redes y de servicios de comunicaciones electrónicas disponibles al público, gestionarán adecuadamente los riesgos de seguridad que puedan afectar a sus redes y servicios a fin de garantizar un adecuado nivel de seguridad y evitar o reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en las redes interconectadas. 2. Asimismo, los operadores de redes públicas de comunicaciones electrónicas garantizarán la integridad de las mismas a fin de asegurar la continuidad en la prestación de los servicios que utilizan dichas redes. 3. Los operadores que exploten redes o presten servicios de comunicaciones electrónicas disponibles al público notificarán al Ministerio de Industria, Energía y Turismo las violaciones de la seguridad o pérdidas de integridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios. Cuando proceda, el Ministerio informará a las autoridades nacionales competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). Asimismo, podrá informar al público o exigir a las empresas que lo hagan, en caso de estimar que la divulgación de la violación reviste interés

seguridad de las redes y de los servicios de comunicaciones electrónicas[195]». Por tanto, los operadores de servicios de comunicaciones electrónicas disponibles al público, están sujetos a dos tipos de obligaciones en relación a la notificación de violación: i) en el primer caso, de datos personales, obligación de notificar a la Agencia Española de Protección de Datos; y, ii) en el segundo caso, de seguridad e integridad de la información, obligación de notificar al Ministerio de Industria, Energía y Turismo[196].

5.2.3 Reglamento Europeo de Protección de Datos

Una de las novedades presentes en el RGPD es la "notificación de una violación de seguridad de los datos personales a la autoridad de control",

---

público. Una vez al año, el Ministerio presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado».

[195] La propia norma nos indica lo que se ha de entender por «servicios de comunicaciones electrónicas», al definirlo en el apartado 35 del Anexo II como «el prestado por lo general a cambio de una remuneración que consiste, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas, con inclusión de los servicios de telecomunicaciones y servicios de transmisión en las redes utilizadas para la radiodifusión, pero no de los servicios que suministren contenidos transmitidos mediante redes y servicios de comunicaciones electrónicas o de las actividades que consistan en el ejercicio del control editorial sobre dichos contenidos; quedan excluidos, asimismo, los servicios de la sociedad de la información definidos en el artículo 1 de la Directiva 98/34/CE que no consistan, en su totalidad o principalmente, en el transporte de señales a través de redes de comunicaciones electrónicas». Entendemos que, en relación a la exclusión de los servicios de la sociedad de la información, en la actualidad, la referencia a la Directiva ha de referirse a la Directiva 2015/1535 del Parlamento Europeo y del Consejo de 9 de septiembre de 2015 por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada). DOUE L/241 17/09/15. Pues bien, en ésta se establece la definición de "servicio" como «todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. A efectos de la presente definición, se entenderá por: i) «a distancia», un servicio prestado sin que las partes estén presentes simultáneamente, ii) «por vía electrónica», un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, iii) «a petición individual de un destinatario de servicios», un servicio prestado mediante transmisión de datos a petición individual. En el anexo I figura una lista indicativa de los servicios no cubiertos por esta definición».

[196] Debemos entender que, en la actualidad, la notificación se llevará a cabo al Ministerio de Energía, Turismo y Agenda Digital. Así se desprende del Real Decreto 415/2016, de 3 de noviembre, por el que se reestructuran los departamentos ministeriales. BOE núm 267, de 4 de noviembre de 2016.

incluida desde el primer borrador del RGPD, pero cuyo contenido ha sufrido diversas modificaciones a lo largo de las diferentes versiones del Texto normativo, hasta quedar finalmente regulado en el artículo 33 RGPD[197]. Sus características principales son:

5.2.3.1 Violación de la seguridad de los datos personales

Como punto inicial, debemos determinar qué entendemos por «violación de la seguridad de los datos personales». La definición se recoge en el apartado 12 del artículo 4 RGPD. A este respecto, entendemos por aquella, «toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos».

Así, sobre el responsable del tratamiento recae la obligación de notificar los incidentes de seguridad que hubieran comprometido la integridad, disponibilidad y seguridad de los datos personales. No obstante, a priori,

---

[197] Así, el artículo 33 declara: «1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. 2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento. 3. La notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información; c) describir las posibles consecuencias de la violación de la seguridad de los datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. 4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. 5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo».

parece que no se detallan de forma clara los supuestos susceptibles de ser considerados «violaciones de la seguridad de los datos personales». El actual texto del RGPD, no viene a desarrollar, de forma precisa, bajo qué supuestos se deberían comunicar las “violaciones de la seguridad de los datos personales”. Con la actual redacción del RGPD, los responsables del tratamiento podrían notificar a la Autoridad de Control cualquier incidencia que hayan gestionado y registrado en sus sistemas de información.

El hecho de no incluir un criterio cualitativo ni cuantitativo sobre el tipo de incidencias o el número de usuarios afectados, puede llevar a que se confundan “simples incidencias” suscitadas en los sistemas de información, sin importar el volumen de afectados, ni de la sensibilidad de los datos involucrados en el incidente, con “violaciones de la seguridad de los datos personales”, y como producto de dicha confusión, no sepa cuándo cumplir con la obligación de comunicación a la Autoridad de Control.

5.2.3.2 Sin dilación indebida

En el RGPD no se detallan cuáles son los supuestos o circunstancias que podrían justificar un retraso o dilación en la notificación de la violación de la seguridad de los datos personales. El concepto «sin dilación indebida» que se establece en el artículo 33.1 RGPD, constituye un concepto jurídico indeterminado, cuyo alcance y significado debe extraerse de la ausencia de una justificación bastante y suficiente, que determine las razones por las cuales no se pone en conocimiento de dicho regulador la incidencia producida en este plazo perentorio establecido expresamente por la normativa.

Llama la atención que el RGPD establezca un límite máximo de tiempo que debe transcurrir desde que se tuvo conocimiento de la violación de la seguridad de los datos personales, hasta la comunicación a la Autoridad de Control. Ahora bien, en la redacción de esta normativa, se indica que dicha

notificación habrá de producirse «sin dilación indebida y, de ser posible a más tardar 72 horas después de que haya tenido constancia de ella»[198].

Afirma SAIZ PEÑA que la imposición de un plazo tan rígido para realizar dicha notificación podría conllevar al incumplimiento de la obligación referida, en la medida en que podrían suscitarse en los que, aun habiendo detectado el incidente, podrían transcurrir varios días sin que sea posible determinar el alcance y los efectos derivados del mismo[199].

Como digo, la actual redacción del RGPD ha flexibilizado el plazo de comunicación de la violación de datos personales, ampliándolo a 72 horas desde que se ha tenido constancia del incidente, añadiendo la posibilidad de demora en la presentación de dicha notificación, siempre que se acompañe de una explicación que justifique dicha dilación. Así lo afirma el Considerando 85 *in fine*, en los siguientes términos: «Si dicha notificación no es posible en el plazo de 72 horas, debe acompañarse de una indicación de los motivos de la dilación, pudiendo facilitarse información por fases sin más dilación indebida».

La doctrina critica este precepto puesto que hubiera sido deseable que en el RGPD se hubieran establecidos criterios para realizar la notificación, en atención al sector en el que desempeña su actividad el responsable del Tratamiento, determinando supuestos de especial aplicación para el

---

198. Debe hacerse notar que el precepto determina el comienzo del cómputo de este plazo no desde el momento de la producción efectiva de dicha brecha de seguridad, sino desde el instante en que «haya tenido constancia de ella», lo que viene a determinar, a la postre, que no exista necesariamente un paralelismo entre la producción de esta incidencia de seguridad y la comunicación que efectivamente se tiene que llevar a cabo con la autoridad de control, a los efectos del debido control sobre la realización de la misma. Por otro lado, la actual redacción del RGPD ha venido a flexibilizar el plazo de comunicación de la violación de la seguridad de los datos personales. La propuesta de la Comisión recogía en el apartado primero del artículo 31 un plazo de 24 horas: «1. En caso de violación de datos personales, el responsable del tratamiento la notificar. a la autoridad de control sin demora injustificada y, de ser posible, a más tardar veinticuatro horas después de que haya tenido constancia de ella. Si no se hace en el plazo de veinticuatro horas, la notificación a la autoridad de control irá acompañada de una justificación motivada».

199 Sáiz Peña, C. A. (2015). La notificación de brechas de seguridad. En Rallo Lombarte A; García Mahamut, R. (dir.): *Hacia un nuevo derecho europeo de protección de datos.* Valencia: Tirant lo Blanch, p. 787.

cumplimiento de esta obligación, tales como: i) gravedad/complejidad del incidente; ii) la tipología de datos comprometidos; iii) el volumen de datos afectados; o iv) los perjuicios ocasionados a los titulares de los datos comprometidos[200].

5.2.3.3 Comunicación del Encargado del tratamiento.

Al encargado del tratamiento le incumbe la obligación de comunicar al responsable del tratamiento las violaciones de la seguridad de los datos personales, a partir del momento en que hubiera tenido constancia de las mismas[201]. La notificación se ha de producir «sin dilación indebida[202]»

5.2.3.4 Contenido de la notificación

El contenido mínimo de la comunicación de la violación de la seguridad de los datos personales que habrá de notificarse a la Autoridad de Control, viene recogido en el artículo 33.3 RGPD.

La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación[203]. En síntesis, el contenido de la notificación deberá referenciar,

---

[200] Sáiz Peña, C. A. (2015). La notificación de brechas de seguridad. En Rallo Lombarte A; García Mahamut, R. (dir.): *Hacia un nuevo derecho europeo de protección de datos.* Valencia: Tirant lo Blanch, p. 787.

[201] Véase el artículo 33.2 RGPD «el encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento».

[202] Hay que plantearse si se podría aplicar con los encargados del tratamiento por analogía, la obligación que se dispone para con los responsables del tratamiento en el artículo 33.1 RGPD. En la actualidad existen un número creciente de servicios de Cloud Computing, donde el proveedor presta servicios a sus clientes a través de su infraestructura y herramientas, alojándose la información en los sistemas del prestador de servicios. Pensemos que este tipo de proveedores de Cloud almacenan y tratan grandes cantidades de información.

[203] Así, el Considerando 86 RGPD afirma que «el responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos

entre otros aspectos: i) la naturaleza de la violación de la seguridad de los datos, incluyendo el número de interesados afectados, así como los datos personales afectados; ii) los datos de contacto del delegado de protección de datos; iii) las posibles consecuencias que se pueden producir a raíz de la violación; y iv) las medidas de subsanación adoptadas.

De este modo, la voluntad del legislador es doble. Por un lado, se desea que la Autoridad de Control tenga conocimiento del incidente que ha afectado a los datos personales. En segundo lugar, se desea tener constancia de las medias de subsanación que se han implementado, para mitigar los efectos derivados del accidente y procurar que éste no vuelva a ocurrir.

5.2.3.5 Documentación de las violaciones de datos personales

Además de la obligación de notificar a la Autoridad de Control las violaciones de datos personales, el responsable del tratamiento deberá documentar cualquier violación de datos personales, en los términos del artículo 33.5 RGPD.

En todo caso, se establece la obligación de proceder a documentar la eventualidad producida, a los efectos de poder acreditar suficientemente, todas las circunstancias que se deriven de la producción de la misma. A tal efecto, deberá indicarse el contexto del incidente, así como los efectos y medidas correctivas adoptadas. Dicho deber de documentación, se considera fundamental a los efectos de poder analizar adecuadamente lo sucedido, y, en su caso, poder investigar, y depurar las responsabilidades derivadas de la producción de tal brecha de seguridad. El objetivo de esta obligación es que la Autoridad de Control disponga de documentación y evidencias que le permitan verificar el cumplimiento de lo dispuesto en dicho artículo.

---

personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación».

5.2.3.6 Comunicación de una violación de la seguridad de los datos personales al interesado

En relación al plazo aplicable para notificar a los particulares, «debe verificarse que la notificación se ha realizado sin dilación indebida teniendo en cuenta, en particular, la naturaleza y gravedad de la violación de la seguridad de los datos personales y sus consecuencias y efectos adversos para el interesado»[204].Por tanto, la notificación se deberá realizar tan pronto como sea razonablemente posible[205].

Tanto en los Considerandos como en su articulado, el RGPD prevé la posibilidad de la realización de una comunicación de la violación de los datos personales producida al propio titular de los datos o interesado. La realización de esta comunicación tiene que ser llevada a cabo con posterioridad a la producida a la Agencia Española de Protección de Datos. Esta obligación surge siempre que la violación de la seguridad de los datos personales afecte negativamente a la protección de datos personales del interesado, o que la misma afecte, al menos, a su ámbito de privacidad. El objetivo de esta comunicación a los particulares afectados por la violación de la seguridad, tiene por objeto permitir a los interesados la oportunidad de mitigar los riesgos de los perjuicios derivados del incidente, mediante la aplicación de medidas adecuadas para impedir que sus datos sigan siendo vulnerados.

Por tanto, el RGPD establece en su artículo 34.1 la comunicación de una violación de la seguridad de los datos personales al interesado, estableciendo su apartado primero que:

> *«Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de*

[204] Así se reconoce expresamente en el Considerando 87 RGPD

[205] Podemos deducir que, una vez notificada la violación de la seguridad de los datos personales a la Autoridad de Control, será ésta quien avale la necesidad de comunicar el incidente a los afectados.

las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida».

La obligación de notificar del artículo 34 RGPD no nace cuando se ha producido una afección a los datos personales del interesado o a la privacidad del mismo, sino que surge cuando la afectación tenga el carácter de probable. No es necesario que se haya producido un daño efectivo contra dichos datos, o contra la privacidad de su titular, ya que esta obligación, tal y como se configura legalmente, está situada en un momento previo, para su activación es suficiente contemplar la posibilidad, y no la consumación de la violación producida a dichos datos.

Esta obligación nace siempre en un momento después, cuando por parte del responsable del tratamiento o el encargado del mismo se haya procedido a comunicar la brecha digital producida a la Autoridad de Control.

Su redacción nos plantea varias dudas. De este modo, ¿quién determina la probabilidad de que la violación entrañe un alto riesgo para los derechos y libertades de las personas físicas? Además, ¿cuán alto ha de ser el riesgo para que se active la obligatoriedad de notificar a las personas físicas de la violación de la seguridad producida? ¿Quién fija todos esos parámetros?

Por otro lado, la comunicación describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y «contendrá al menos, la información y las medidas reflejadas en los apartados b), c) y d) del artículo 33 RGPD»[206]. Aquella no será necesaria si se cumple alguna de las siguientes condiciones[207]:

– El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado

---

[206] Véase el artículo 34.2 RGPD in fine. La información a la que hace referencia es: i) el nombre y los datos de contacto del delegado de protección de datos; ii) descripción de las posibles consecuencias de la violación de la seguridad de los datos personales; iii) descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

[207] Véase el artículo 34.3 RGPD.

a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado.

– El responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado.
– Suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

En todo caso, no debe pasarse por alto la facultar que tiene la propia Agencia Española de Protección de Datos de poder verificar la efectiva aplicación de las medidas adoptadas, y que, a su criterio, si lo juzga conveniente en caso de necesidad, puede ordenar la realización de dicha notificación al titular de los datos afectados, a los efectos de una mejor preservación de su derecho a la privacidad.

5.2.4 Ley de servicios de la sociedad de la información y de comercio electrónico.

La LGTel introduce una disposición final segunda por la que se modifica la LSSI[208], introduce una disposición adicional novena en ésta, con el fin de regular la gestión de incidentes de ciberseguridad que afecten a la red de Internet[209].

---

[208] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE núm 166, de 12/07/2002.

[209] De este modo, la Ley 34/2002, en su Disposición adicional novena, relativa a la gestión de incidentes de ciberseguridad que afecten a la red de Internet, establece expresamente que «1. Los prestadores de servicios de la Sociedad de la Información, los registros de nombres de dominio y los agentes registradores que estén establecidos en España están obligados a prestar su colaboración con el CERT competente, en la resolución de incidentes de ciberseguridad que afecten a la red de Internet y actuar bajo las recomendaciones de seguridad indicadas o que sean establecidas en los códigos de conducta que de esta Ley se deriven. Los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad colaborarán con las autoridades competentes para la aportación de las evidencias técnicas necesarias para la persecución

de los delitos derivados de dichos incidentes de ciberseguridad. 2. Para el ejercicio de las funciones y obligaciones anteriores, los prestadores de servicios de la Sociedad de la información, respetando el secreto de las comunicaciones, suministrarán la información necesaria al CERT competente, y a las autoridades competentes, para la adecuada gestión de los incidentes de ciberseguridad, incluyendo las direcciones IP que puedan hallarse comprometidas o implicadas en los mismos. De la misma forma, los órganos, organismos públicos o cualquier otra entidad del sector público que gestionen equipos de respuesta a incidentes de seguridad podrán intercambiar información asociada a incidentes de ciberseguridad con otros CERTs o autoridades competentes a nivel nacional e internacional, siempre que dicha información sea necesaria para la prevención de incidentes en su ámbito de actuación. 3. El Gobierno pondrá en marcha, en el plazo de seis meses, un programa para impulsar un esquema de cooperación público-privada con el fin de identificar y mitigar los ataques e incidentes de ciberseguridad que afecten a la red de Internet en España. Para ello, se elaborarán códigos de conducta en materia de ciberseguridad aplicables a los diferentes prestadores de servicios de la sociedad de la información, y a los registros de nombres de dominio y agentes registradores establecidos en España. Los códigos de conducta determinarán el conjunto de normas, medidas y recomendaciones a implementar que permitan garantizar una gestión eficiente y eficaz de dichos incidentes de ciberseguridad, el régimen de colaboración y condiciones de adhesión e implementación, así como los procedimientos de análisis y revisión de las iniciativas resultantes. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información coordinará las actuaciones que se pongan en marcha derivadas de estos códigos de conducta. 4. Conforme a los códigos de conducta que se definan en particular, los prestadores de servicios de la sociedad de la información deberán identificar a los usuarios afectados por los incidentes de ciberseguridad que les sean notificados por el CERT competente, e indicarles las acciones que deben llevar a cabo y que están bajo su responsabilidad, así como los tiempos de actuación. En todo caso, se les proporcionará información sobre los perjuicios que podrían sufrir u ocasionar a terceros si no colaboran en la resolución de los incidentes de ciberseguridad a que se refiere esta disposición. En el caso de que los usuarios no ejerciesen en el plazo recomendado su responsabilidad en cuanto a la desinfección o eliminación de los elementos causantes del incidente de ciberseguridad, los prestadores de servicios deberán, bajo requerimiento del CERT competente, aislar dicho equipo o servicio de la red, evitando así efectos negativos a terceros hasta el cese de la actividad maliciosa. El párrafo anterior será de aplicación a cualquier equipo o servicio geolocalizado en España o que esté operativo bajo un nombre de dominio «.es» u otros cuyo Registro esté establecido en España. 5. Reglamentariamente se determinará los órganos, organismos públicos o cualquier otra entidad del sector público que ejercerán las funciones de equipo de respuesta a incidentes de seguridad o CERT competente a los efectos de lo previsto en la presente disposición. 6. La Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información garantizará un intercambio fluido de información con la Secretaría de Estado de Seguridad del Ministerio del Interior sobre incidentes, amenazas y vulnerabilidades según lo contemplado en la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas. En este sentido se establecerán mecanismos de coordinación entre ambos órganos para garantizar la provisión de una respuesta coordinada frente a incidentes en el marco de la presente Ley.»

5.2.5 Directiva sobre privacidad y las comunicaciones electrónicas

La conocida como Directiva sobre privacidad y las comunicaciones electrónicas[210] fue modificada por la Directiva 2009/136/CE[211] con el objeto de actualizar su contenido pues existía una preocupación creciente tanto por el despliegue de las nuevas redes digitales, ya que poseen gran capacidad y muchas posibilidades en materia de tratamiento de los datos personales, así como por los nuevos servicios de comunicaciones electrónicas disponibles al público a través de Internet, pues «introducen nuevas posibilidades para los usuarios, pero también nuevos riesgos para sus datos personales y su intimidad»[212].

De este modo, se introduce en su articulado la definición de «violación de los datos personales»[213], y se añaden, en relación al tema que nos preocupa, diferentes apartados al artículo 4 en relación a la seguridad de los servicios de comunicaciones electrónicas disponibles al público a través de Internet, con el fin de establecer la obligación de notificar tanto a la autoridad nacional competente, como al propio abonado o particular afectado, por parte del

---

[210] Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) DOCE L 201 de 31.07.2002

[211] Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n o 2006/2004 sobre la cooperación en materia de protección de los consumidores. DOUE L 337, de 18.12.2009

[212] Al respecto, véase los Considerandos 5 y 6 de la Directiva 2002/58/CE

[213] Así, esta norma entiende por «violación de los datos personales» toda violación de la seguridad que provoque la destrucción, accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, de datos personales transmitidos, almacenados o tratados de otro modo en relación con la prestación de un servicio de comunicaciones electrónicas de acceso público en la Comunidad.

proveedor de estos servicios, cuando se produzca una violación de los datos personales[214].

5.2.6 Reglamento 611/2013 relativo a las medidas aplicables a la notificación de casos de violación de datos personales

El objeto principal de este Reglamento[215] es regular el fenómeno del data breach o violaciones de datos personales. En él, se diferencia la obligación de la notificación a la Autoridad Nacional competente, y la notificación al abonado o particular.

La obligación de notificar una violación de datos deviene obligatoria para los proveedores de comunicaciones electrónicas en virtud del Reglamento 611/2013 de la Comisión relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE.

---

[214] La obligación de la notificación aparece reflejada en artículo 4.3 de la Directiva 2002/58/CE. «En caso de violación de los datos personales, el proveedor de los servicios de comunicaciones electrónicas disponibles al público notificará, sin dilaciones indebidas, dicha violación a la autoridad nacional competente. Cuando la violación de los datos personales pueda afectar negativamente a la intimidad o a los datos personales de un abonado o particular, el proveedor notificará también la violación al abonado o al particular sin dilaciones indebidas. La notificación de una violación de los datos personales a un abonado o particular afectado no será necesaria si el proveedor ha probado a satisfacción de la autoridad competente que ha aplicado las medidas de protección tecnológica convenientes y que estas medidas se han aplicado a los datos afectados por la violación de seguridad. Unas medidas de protección de estas características convierten los datos en incomprensibles para toda persona que no esté autorizada a acceder a ellos. Sin perjuicio de la obligación del proveedor de informar a los abonados o particulares afectados, si el proveedor no ha notificado ya al abonado o al particular la violación de los datos personales, la autoridad nacional competente podrá exigirle que lo haga, una vez evaluados los efectos adversos posibles de la violación. La notificación al abonado o al particular describirá al menos la naturaleza de la violación de los datos personales y los puntos de contacto donde puede obtenerse más información, y recomendará medidas para atenuar los posibles efectos adversos de dicha violación. La notificación a la autoridad nacional competente describirá, además, las consecuencias de la violación y las medidas propuestas o adoptadas por el proveedor respecto a la violación de los datos personales».

[215] Reglamento 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas. DOUE L 173, de 26.06.2013

En primer lugar, en relación a la notificación a la autoridad nacional competente, la novedad más relevante es la existencia de un plazo de 24 horas para realizar la notificación, cuando sea posible, desde la detección del incidente[216].

En segundo lugar, también se recoge la obligación de notificar al abonado o particular[217]. No obstante, esta obligación de notificar al abonado o particular

---

[216] En concreto, el artículo 2 establece: «1. Los proveedores notificarán todos los casos de violación de datos personales a la autoridad nacional competente. 2. En la medida de lo posible, los proveedores notificarán los casos de violación de datos personales a la autoridad nacional competente dentro de las 24 horas siguientes a la detección del caso. Los proveedores consignarán en su notificación a la autoridad nacional competente la información recogida en el anexo I. Se considerará que se ha detectado un caso de violación de datos personales cuando el proveedor tenga conocimiento suficiente de que se ha producido un incidente de seguridad que compromete datos personales para efectuar una notificación válida conforme a lo establecido en el presente Reglamento. 3. Cuando no se disponga de toda la información indicada en el anexo I y sea preciso investigar más exhaustivamente el caso de violación de datos personales, se autorizará al proveedor a enviar una notificación inicial a la autoridad nacional competente dentro de las 24 horas siguientes a la detección del caso. Esta notificación inicial incluirá la información contemplada en el anexo I, sección 1. El proveedor remitirá una segunda notificación a la autoridad nacional competente lo antes posible y, a más tardar, dentro de los tres días siguientes a la notificación inicial. En esta segunda notificación se incluirá la información indicada en el anexo I, sección 2, y, cuando proceda, se actualizará la información ya proporcionada. Cuando, a pesar de las pesquisas realizadas, el proveedor no pueda proporcionar toda la información en el plazo de los tres días siguientes a la notificación inicial, deberá notificar toda la información de que disponga dentro de ese plazo y presentar a la autoridad nacional competente una justificación motivada de la tardía notificación de la información restante. El proveedor notificará esa información restante a la autoridad nacional competente y, cuando proceda, actualizará la información ya proporcionada, en el plazo más breve posible. 4. La autoridad nacional competente pondrá a disposición de todos los proveedores establecidos en el Estado miembro de que se trate un soporte electrónico seguro para notificar los casos de violación de datos personales, así como información sobre los procedimientos para acceder a dicho soporte y utilizarlo. Cuando sea necesario, la Comisión convocará reuniones con las autoridades nacionales competentes a fin de facilitar la aplicación de esta disposición. 5. Cuando una violación de datos personales afecte a abonados o particulares de Estados miembros distintos de aquel de la autoridad nacional competente a la que se haya notificado el caso de violación de datos personales, la autoridad nacional competente informará a las demás autoridades nacionales afectadas. A fin de facilitar la aplicación de esta disposición, la Comisión elaborará y mantendrá al día una lista de las autoridades nacionales competentes y los puntos de contacto correspondientes».

[217] Su artículo 3 expresamente reconoce «1. Cuando un caso de violación de datos personales pueda afectar negativamente a los datos personales o a la intimidad de un abonado o particular, el proveedor, además de remitir la notificación contemplada en el artículo 2, también notificará el caso al abonado o particular. 2. Se evaluará si un caso de violación de datos personales puede afectar negativamente a los datos personales o a la intimidad de un abonado o particular atendiendo, en particular, a las siguientes circunstancias: a) la naturaleza y el contenido de los datos personales en cuestión, en

afectado, no será necesaria si el proveedor ha podido probar ante la autoridad nacional competente que ha aplicado las medidas tecnológicas de protección convenientes y que se han aplicado a los datos afectados por la violación de seguridad. Estas medidas de protección convertirán los datos en incomprensibles para todas aquellas personas que no estén autorizadas a acceder a ellos[218].

---

particular si se trata de datos financieros, de categorías especiales de datos contempladas en el artículo 8, apartado 1, de la Directiva 95/46/CE, así como de datos de localización, registros de internet, historiales de navegación en internet, datos de correo electrónico y listas de llamadas detalladas; b) las posibles consecuencias de la violación de datos personales para el abonado o particular afectado, en particular cuando la violación pueda entrañar fraude o usurpación de identidad, daños físicos, sufrimiento psicológico, humillación o perjuicio para su reputación; c) las circunstancias en que se haya producido la violación de datos personales, teniendo en cuenta, en particular, el lugar en que hayan sido robados los datos o el momento en que el proveedor haya tenido conocimiento de que los datos se hallan en poder de un tercero no autorizado. 3. La notificación al abonado o particular se efectuará sin dilación injustificada tras haberse detectado la violación de datos personales, tal y como se establece en el artículo 2, apartado 2, párrafo tercero. Dicha notificación no dependerá de la notificación de la violación de datos personales a la autoridad nacional competente mencionada en el artículo 2. 4. El proveedor incluirá en su notificación al abonado o particular la información establecida en el anexo II. La notificación al abonado o particular se redactará en un lenguaje claro y fácilmente comprensible. El proveedor no deberá valerse de la notificación para promover o anunciar servicios nuevos o adicionales. 5. En circunstancias excepcionales, cuando la notificación al abonado o particular pueda comprometer la investigación del caso de violación de datos personales, el proveedor podrá, previa autorización de la autoridad nacional competente, demorar la notificación al abonado o particular hasta que la autoridad nacional competente considere que puede notificarse la violación de datos personales de conformidad con el presente artículo. 6. El proveedor notificará la violación de datos personales al abonado o particular por vías de comunicación que garanticen una pronta recepción de la información y sean seguras con arreglo al estado actual de la técnica. La información sobre el caso se referirá exclusivamente a este y no se adjuntará a información sobre otros asuntos. 7. Cuando, pese a haber hecho todo lo posible, el proveedor que tenga una relación contractual directa con el usuario final no pueda identificar en el plazo a que hace referencia el apartado 3 a todos los particulares que puedan verse perjudicados por la violación de datos personales, podrá notificarles esa información insertando anuncios en los principales medios de comunicación nacionales o regionales de los Estados miembros en cuestión dentro del citado plazo. Tales anuncios contendrán la información indicada en el anexo II, si procede de forma resumida. En este caso, el proveedor seguirá haciendo todo lo posible para identificar a dichos particulares y notificarles la información contemplada en el anexo II lo antes posible».

[218] No estamos ante una medida novedosa. Se ha de tener en cuenta que en el ámbito de las telecomunicaciones existe la posibilidad de proteger mediante procedimientos de cifrado cualquier tipo de información que se transmita por las redes. Así lo establece expresamente el artículo 43.1 de la LGTel, al igual que lo establecía la normativa sectorial desde 1988. Véase el apartado primero del

A destacar, la obligación existente por parte de la autoridad nacional competente de informar de la existencia de la violación de datos personales a las demás autoridades nacionales afectadas. Así lo establece, como hemos tenido ocasión de poner de manifiesto, el apartado 5 del artículo 2 del Reglamento comentado.

5.2.7 Directiva de seguridad en las redes y sistemas de información

Expresamente se determina en el Considerando 4 de la Directiva (UE) 2016/1148[219] que «los operadores de servicios esenciales y los proveedores de servicios digitales deben estar sujetos a requisitos en materia de seguridad y notificación de incidentes, con el fin de fomentar una cultura de gestión de riesgos y garantizar que se informe de los incidentes más graves». Sin embargo, se debe destacar, el carácter subsidiario[220] de su aplicación, tal y como se refleja en el Considerando 9 de la misma.

Se debe destacar el hecho de centralizar la recepción de todas las notificaciones de los incidentes en las Autoridades Competentes o en los equipos de respuesta a incidentes de seguridad informática. Los puntos de contacto únicos no deben recibir directamente ninguna notificación de incidente, salvo en caso de que actúen también como autoridad competente o como equipos de respuesta a incidentes de seguridad informática[221].Para

---

artículo 52 de la LGTel 1998, y el apartado primero del artículo 36 de la LGTel 2003. Ambas normas derogadas por la normativa del año 2014.

[219] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. DOUE L194 19.07.2016

[220] Como bien reconoce en su Considerando 9, «determinados sectores de la economía ya están ya regulados o pueden regularse en el futuro mediante actos jurídicos sectoriales de la Unión que incluyan normas relacionadas con la seguridad de las redes y sistemas de información. Siempre que esos actos jurídicos de la Unión contengan disposiciones por las que se impongan requisitos en materia de seguridad de las redes y sistemas de información o en materia de notificación de incidentes, dichas disposiciones deben aplicarse en lugar de las disposiciones correspondientes de la presente Directiva si contienen requisitos cuyos efectos sean, como mínimo, equivalentes a los de las obligaciones que establece la presente Directiva».

[221] Véase el Considerando 32 de la Directiva (UE) 2016/1148.

garantizar que la información se facilite efectivamente a los Estados miembros y a la Comisión, el punto de contacto único debe presentar un informe resumido al Grupo de cooperación, y este debe estar anonimizado. Se detalla en el Considerando 33 de la Directiva (UE) 2016/1148 que el informe resumido debe contener información sobre el número de notificaciones recibidas y sobre las características de los incidentes notificados, como los tipos de vulneraciones de la seguridad, su gravedad o su duración».

Las Autoridades Competentes deben procurar que se mantengan los canales de intercambio de información informales y de confianza. Antes de dar publicidad a los incidentes notificados a las autoridades competentes, es preciso sopesar debidamente el interés de los ciudadanos en ser informados sobre amenazas que en términos comerciales y de reputación puedan sufrir los operadores de servicios esenciales y los proveedores de servicios digitales que notifican incidentes[222].

A la hora de determinar los requisitos que se han de seguir en materia de seguridad y notificación de incidentes, la regulación de la Directiva (UE) 2016/1148 distingue el tipo de operador de servicios que ha sufrido el incidente[223]. De este modo, el Capítulo IV se dedica de la seguridad de las redes y sistemas de información de los operadores de servicios

[222] Véase el Considerando 59 de la Directiva (UE) 2016/1148.

[223] La definición del término incidente aparece recogida en el apartado 7) del artículo 4 de la Directiva (UE) 2016/1148 como «todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información».

esenciales[224], y el Capítulo V se dedica de la seguridad de las redes y sistemas de información de los operadores de servicios digitales[225].

Por tanto, y en relación a los operadores de servicios esenciales, el artículo 14 de la Directiva (UE) 2016/1148 establece que los Estados miembros velarán por que los operadores de servicios esenciales tomen las medidas técnicas y de organización adecuadas y proporcionadas para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información que utilizan en sus operaciones. Habida cuenta de la situación, dichas medidas garantizarán un nivel de seguridad de las redes y sistemas de información adecuado en relación con el riesgo planteado. Además, aquellos velarán por que los operadores de servicios esenciales notifiquen sin dilación indebida a la autoridad competente, o al equipo de respuesta a incidentes de seguridad informática, los incidentes que tengan efectos significativos en la continuidad de los servicios esenciales que prestan.

---

224 El artículo 4 de la Directiva (UE) 2016/1148 se encarga de definir el término de «operador de servicios esenciales». Así, el apartado 7) del mismo lo define como «una entidad pública o privada de uno de los tipos que figuran en el anexo II, que reúna los criterios establecidos en el artículo 5, apartado 2». Como bien se afirma en la definición, estos criterios son: «a) una entidad presta un servicio esencial para el mantenimiento de actividades sociales o económicas cruciales; b) la prestación de dicho servicio depende de las redes y sistemas de información, y c) un incidente tendría efectos perturbadores significativos en la prestación de dicho servicio».

225 La definición de «proveedor de servicios digitales» es mucho más sencilla. El apartado 6) del artículo 4 de la Directiva (UE) 2016/1148 considera de este modo a «toda persona jurídica que preste un servicio digital». Este último es «un servicio en el sentido del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo, de 9 de septiembre de 2015, por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (DO L 241 de 17.9.2015, p. 1[1.A efectos de la presente Directiva, se entenderá por: … b) «servicio»:todo servicio de la sociedad de la información, es decir, todo servicio prestado normalmente a cambio de una remuneración, a distancia, por vía electrónica y a petición individual de un destinatario de servicios. A efectos de la presente definición, se entenderá por: i) «a distancia», un servicio prestado sin que las partes estén presentes simultáneamente, ii) «por vía electrónica», un servicio enviado desde la fuente y recibido por el destinatario mediante equipos electrónicos de tratamiento (incluida la compresión digital) y de almacenamiento de datos y que se transmite, canaliza y recibe enteramente por hilos, radio, medios ópticos o cualquier otro medio electromagnético, iii) «a petición individual de un destinatario de servicios», un servicio prestado mediante transmisión de datos a petición individual]), que sea de uno de los tipos que figuran en el anexo III.

Estas notificaciones incluirán información que permita determinar cualquier efecto transfronterizo del incidente.

Continúa el artículo indicando que, para determinar la importancia de los efectos de un incidente, se tendrán en cuenta, en particular, los siguientes parámetros: a) el número de usuarios afectados por la perturbación del servicio esencial; b) la duración del incidente; c) la extensión geográfica con respecto a la zona afectada por el incidente. De este modo, sobre la base de la información proporcionada en la notificación por el operador de servicios esenciales, la Autoridad Competente o el equipo de respuesta a incidentes de seguridad informática, informará al otro u otros Estados miembros afectados acerca de si el incidente tiene efectos significativos en la continuidad de los servicios esenciales en dicho Estado miembro. Al hacer esto, se deberá mantener la seguridad y los intereses comerciales del operador de servicios esenciales, así como la confidencialidad de la información proporcionada en su notificación.

Una vez consultado al operador de servicios esenciales notificante, la autoridad competente o el equipo de respuesta a incidentes de seguridad informática podrán informar al público sobre determinados incidentes, cuando la concienciación pública sea necesaria para evitar un incidente o gestionar uno que ya se haya producido

En lo que atañe a los operadores de servicios digitales, se ha de empezar por el final, y es que el artículo 16.11 de la Directiva (UE) 2016/1148 establece una salvaguarda[226] en la aplicación del Capítulo V. Por otro lado, y entrando en los requisitos, indicar que el artículo 16.1 de la Directiva (UE) 2016/1148 establece que «los Estados miembros velarán por que los proveedores de servicios digitales determinen y adopten medidas técnicas y

---

[226] Expresamente se determina que «el presente capítulo no se aplicará a las microempresas y pequeñas empresas tal como se definen en la Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de 20.5.2003 [en ésta su artículo 2.1 reconoce que «la categoría de microempresas, pequeñas y medianas empresas (PYME) está constituida por las empresas que ocupan a menos de 250 personas y cuyo volumen de negocios anual no excede de 50 millones de euros o cuyo balance general anual no excede de 43 millones de euros»]).

organizativas adecuadas y proporcionadas para gestionar los riesgos existentes para la seguridad de las redes y sistemas de información que se utilizan en el marco de la oferta de servicios en la Unión a que se refiere el anexo III. Habida cuenta de los avances técnicos, dichas medidas garantizarán un nivel de seguridad de las redes y los sistemas de información adecuado en relación con el riesgo planteado, y tendrán en cuenta lo siguiente: a) la seguridad de los sistemas e instalaciones; b) la gestión de incidentes; c) la gestión de la continuidad de las actividades; d) la supervisión, auditorías y pruebas; e) el cumplimiento de las normas internacionales».

Los Estados miembros velarán por que los proveedores de servicios digitales notifiquen sin dilación indebida a la autoridad competente o al equipo de respuesta a incidentes de seguridad informática, cualquier incidente que tenga un impacto significativo en la prestación de uno de los servicios a que se refiere el anexo III que ellos ofrezcan en la Unión. Las notificaciones incluirán la información necesaria para que la autoridad competente o el equipo de respuesta a incidentes de seguridad informática, puedan determinar la importancia de cualquier impacto transfronterizo.

Para determinar si el impacto de un incidente es significativo se tendrán en cuenta, en particular, los siguientes parámetros: a) el número de usuarios afectados por el incidente, en particular los usuarios que dependen del servicio para la prestación de sus propios servicios; b) la duración del incidente; c) la extensión geográfica con respecto a la zona afectada por el incidente; d) el grado de perturbación del funcionamiento del servicio; e) el alcance del impacto sobre las actividades económicas y sociales.

La obligación de la notificación del incidente únicamente se aplicará cuando el proveedor de servicios digitales tenga acceso a la información necesaria para valorar el impacto de un incidente en función de los siguientes parámetros: a) la seguridad de los sistemas e instalaciones; b) la gestión de incidentes; c) la gestión de la continuidad de las actividades; d) la supervisión, auditorías y pruebas; e) el cumplimiento de las normas internacionales.

Si el incidente afecta a dos o varios Estados miembros, la autoridad o el equipo de respuesta a incidentes de seguridad informática al que se haya notificado el incidente, informará del mismo a los demás Estados miembros afectados. Al hacerlo, se preservará, la seguridad y los intereses comerciales del proveedor de servicios digitales, así como la confidencialidad de la información facilitada.

Tras consultar al proveedor de servicios digitales afectado, la autoridad competente o el equipo de respuesta a incidentes de seguridad informática al que se le haya notificado el incidente y, en su caso, las autoridades o el equipo de respuesta a incidentes de seguridad informática de los demás Estados miembros afectados, podrán informar al público de determinados incidentes o exigir al proveedor de servicios digitales que lo haga, cuando el conocimiento del público sea necesario para evitar un incidente o hacer frente a un incidente en curso, o cuando la divulgación de un incidente redunde en interés público.

Por último, y para completar el círculo, la Directiva (UE) 2016/1148 afirma que las entidades que no hayan sido identificadas como operadores de servicios esenciales y no sean proveedores de servicios digitales podrán notificar voluntariamente los incidentes que tengan efectos significativos en la continuidad de los servicios que prestan. En este caso, cuando tramiten las notificaciones, los Estados miembros actuarán de conformidad con el procedimiento establecido en el artículo 14. Esta notificación voluntaria no dará lugar a la imposición a la entidad notificante de obligaciones a las que no estaría sujeta de no haberse producido dicha notificación.

5.2.8 Propuesta de Directiva por la que se establece el Código Europeo de las Comunicaciones Electrónicas

A la hora de revisar el marco regulador de las comunicaciones electrónicas por parte de la Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones

Electrónicas[227], se comprueba que también resulta afectada la regulación de la seguridad de las redes y servicios[228].

[227] Véase COM(2016) 590 final de 12.10.2016 Texto completo accesible en el siguiente link http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CONSIL:ST_9355_2017_INIT&from=EN

[228] En este sentido, expresamente se indica por parte del artículo 40 relativo a las redes y los servicios «1. Los Estados miembros velarán por que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público adopten las medidas técnicas y organizativas adecuadas para gestionar adecuadamente los riesgos existentes para la seguridad de sus redes y servicios. Considerando el estado de la técnica, dichas medidas garantizarán un nivel de seguridad adecuado al riesgo presente. En particular, se adoptarán medidas para evitar y reducir al mínimo el impacto de los incidentes de seguridad en los usuarios y en otras redes y servicios. 2. Los Estados miembros velarán por que las empresas que suministran redes de públicas comunicaciones adopten todas las medidas oportunas para garantizar la integridad de sus redes a fin de asegurar la continuidad de la prestación de los servicios que utilizan esas redes. 3. Los Estados miembros velarán por que las empresas que suministran redes públicas de comunicaciones o prestan servicios de comunicaciones electrónicas disponibles para el público notifiquen sin tardanza a la autoridad competente las violaciones de la seguridad que hayan tenido un impacto significativo en la explotación de las redes o los servicios. Con el fin de determinar la importancia del impacto de un incidente en materia de seguridad, se tendrán en cuenta, en particular, los parámetros siguientes: a) el número de usuarios afectados por la violación; b) la duración de esta; c) el área geográfica afectada; d) la medida en que se ha perturbado el funcionamiento del servicio; e) el impacto sobre las actividades económicas y sociales. Cuando proceda, la autoridad competente afectada informará a las autoridades competentes de otros Estados miembros y a la Agencia Europea de Seguridad en las Redes y la Información (ENISA). La autoridad de que se trate podrá informar al público o exigir a las empresas que lo hagan, en caso de estimar que la divulgación de la violación reviste interés público. Una vez al año, la autoridad competente correspondiente presentará a la Comisión y a la ENISA un informe resumido sobre las notificaciones recibidas y las medidas adoptadas de conformidad con este apartado. 4. El presente artículo se entenderá sin perjuicio del Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y de la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas. 5. La Comisión será habilitada para adoptar actos delegados de conformidad con el artículo 109 con objeto de especificar las medidas a que se refieren los apartados 1 y 2».

5.2.9 Propuesta de Reglamento sobre el tratamiento de datos personales por las instituciones, órganos y organismos de la Unión

Esta Propuesta de Reglamento[229], que está llamada a derogar el Reglamento CE núm. 45/2001, reconoce que «los actos jurídicos adoptados con arreglo a los Tratados o las normas internas de las instituciones y organismos de la Unión pueden imponer limitaciones a […] la comunicación de una violación de la seguridad de los datos personales a un interesado […], en la medida en que sea necesario y proporcionado en una sociedad democrática para salvaguardar la seguridad pública, la prevención, investigación y el enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a las amenazas contra la seguridad pública, incluida la protección de la vida humana, especialmente en respuesta a catástrofes naturales o de origen humano, la seguridad interna de las instituciones y organismos de la Unión, otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un importante interés económico o financiero de la Unión o de un Estado miembro, el mantenimiento de registros públicos por razones de interés público general o la protección del interesado o de los derechos y libertades de otros, incluida la protección social, la salud pública y los fines humanitarios»[230].

---

[229] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE COM(2017) 08 final, de 10.01.2017. http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

[230] Véase el Considerando 37 de la Propuesta de Reglamento.

Asimismo, la notificación por parte del responsable del tratamiento de los datos personales, se reconoce en los artículos 37[231] y 38[232], estableciendo la

[231] La Propuesta reconoce en su artículo 37 la obligación de notificar cuando se haya producido una violación de la seguridad de los datos personales al Supervisor Europeo de Protección de Datos, en los siguientes términos «1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará al Supervisor Europeo de Protección de Datos sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación al Supervisor Europeo de Protección de Datos no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. 2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento. 3. La notificación contemplada en el apartado 1 deberá, como mínimo: a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados; b) comunicar el nombre y los datos de contacto del delegado de protección de datos; c) describir las posibles consecuencias de la violación de datos personales; d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos. 4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida. 5. El responsable del tratamiento informará al delegado de protección de datos acerca de la violación de la seguridad de los datos».

[232] La Propuesta reconoce en su artículo 38 la obligación de notificar cuando se haya producido una violación de la seguridad de los datos personales al interesado, en los siguientes términos: «1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida. 2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 37, apartado 3, letras b), c) y d). 3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes: a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado; b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1; c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados. 4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, el Supervisor Europeo de Protección de Datos, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3».

obligación de notificar al Supervisor Europeo de Protección de Datos y al interesado, respectivamente, y reconociendo la obligación por parte del delegado de protección de datos, de ofrecer el asesoramiento que se le solicite acerca de la necesidad de notificar o comunicar el hecho de que haya acaecido una violación de la seguridad de los datos personales.

5.2.10 Propuesta de Reglamento sobre la privacidad y las comunicaciones electrónicas

Por último, me gustaría hacer mención brevemente a la Propuesta de Reglamento presentada por la Comisión por el que se derogará la Directiva 2002/58/CE[233] pues en su artículo 17, relativo a la información sobre los riesgos de seguridad detectados, reconoce expresamente la obligación para el proveedor de servicios:

> *«En caso de que exista un riesgo concreto que pueda comprometer la seguridad de las redes y los servicios de comunicaciones electrónicas, el proveedor del servicio de comunicaciones electrónicas de que se trate informará a los usuarios finales de dicho riesgo y, cuando este quede fuera del ámbito de las medidas que debe adoptar el proveedor de servicios, informará a los usuarios finales de las posibles soluciones, con una indicación de los posibles costes».*

[233] Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) COM(2017) 10 final, de 10.01.2017, y que actualmente se encuentra en la fase de presentación de enmiendas por parte de las distintas comisiones del Parlamento Europeo. Se trata del procedimiento 2017/0003(COD). Texto accesible en el siguiente link http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0010&from=EN

5.3 El daño reputacional en las organizaciones obligadas a la notificación por ser víctimas de una violación de seguridad

La notificación de las brechas a la Autoridad de Control implica un impacto reputacional muy importante en las compañías atacadas por la desconfianza que generan, y que se verán afectadas ante sus clientes, su competencia, sus accionistas y el propio mercado en general. La prensa suele hacerse eco de este tipo de fugas o ataques a datos o sistemas de información de compañías. El conocimiento por el mercado a través de los medios de comunicación de los problemas de seguridad que ha podido tener una compañía u organismo público, tiene un impacto reputacional muy importante en dichas organizaciones.

Afirma SÁIZ PEÑA[234] que sería conveniente reflexionar sobre la forma de establecer este canal de comunicación con la Autoridad de Control, debiendo fomentar por un lado que las empresas atacadas comuniquen sus brechas de seguridad a la Autoridad, pero a la vez intentando dar unas ciertas garantías de confidencialidad para evitar que sean filtrados a la prensa o que sea un listado público consultable por cualquiera, de cara a que se pueda minimizar el impacto reputacional que aquello puede conllevar. Resultará fundamental encontrar un equilibrio para que las empresas afectadas no eviten cumplir esta obligación por miedo al daño reputaciones que la notificación de la brecha les puede acarrear

Por otro lado, la notificación de las brechas a la autoridad de control puede implicar una especie de auto denuncia por parte de la compañía, si le fuera atribuible alguna responsabilidad al no haber frenado el ataque, que puede acabar en algunos casos con la apertura de un procedimiento sancionador, sin saber si el hecho de haber cumplido con la propia comunicación servirá de atenuante o no.

---

[234] Sáiz Peña, C. A. (2015). La notificación de brechas de seguridad. En Rallo Lombarte A; García Mahamut, R. (dir.): *Hacia un nuevo derecho europeo de protección de datos.* Valencia: Tirant lo Blanch, p. 813.

Si la autoridad quiere saber exactamente qué ha ocurrido, la normativa podría regular o valorar la posibilidad de entregar un informe de un tercero independiente que establezca qué ha ocurrido en los sistemas de información aportando las correspondientes evidencias electrónicas.

CAPÍTULO IIº: EL PRINCIPIO DEL CONSENTIMIENTO EN EL DERECHO DE PROTECCIÓN DE DATOS

SUMARIO: 1 EL CONSENTIMIENTO.–1.1 La información y el consentimiento del interesado.–1.2 El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico.–1.3 El consentimiento del interesado.–1.4 Licitud del tratamiento y condiciones del consentimiento.–1.5 Formas de prestar el consentimiento.–1.6 Salvaguarda y límites al poder de disposición del titular de los datos.–1.7 Retirada / Revocación del Consentimiento.–1.8 Consentimiento del menor.–1.9 Categorías especiales de datos personales.–1.10 Conclusiones.–2 EL MITO DEL CONSENTIMIENTO Y EL FRACASO DEL MODELO INDIVIDUALISTA DE PROTECCIÓN DE DATOS.–2.1 La ambivalencia del consentimiento.–2.2 El mantra del control.–2.3 El consentimiento en la cultura de protección de datos.–2.4 La limitada virtualidad del consentimiento en los tratamientos de datos de carácter personal en Internet.–2.5 Consentimiento «libre» en una relación «desequilibrada»: el interés legítimo.–2.6 Desinformar informando y el «user empowerment».–2.7 Profiling automatizado.–3 COMPUTACIÓN UBICUA, PRIVACIDAD Y PROTECCIÓN DE DATOS: OPCIONES Y LIMITACIONES PARA RECONCILIAR CONTRADICCIONES SIN PRECEDENTES.–3.1 Introducción.–3.2 Retos a los que nos enfrentamos en materia de privacidad.–3.3 Contradicciones con los fundamentos actuales de la privacidad.–3.4 Propuestas para superar las contradicciones.

1 EL CONSENTIMIENTO

Acertadamente, señalan OLIVER LALANA y MUÑOZ SORO que sobre el papel, lo único que legitima un tratamiento de información personal, salvo que una ley disponga de otra cosa, es la voluntad libre e inequívoca de su titular. Idealmente, con ello se pretende que la información sobre una persona sea procesada solo cuando, como y para los fines que ella quiera. El consentimiento es, así, una de las vías principales que la legislación utiliza para proporcionar a todo individuo un control razonablemente amplio sobre su información[235].

[235] Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi, p. 154.

1.1 La información y el consentimiento del interesado

El artículo 5[236] LOPD proclama la existencia de un derecho de información por parte del interesado en el momento en que se produce una solicitud de sus datos. Este derecho a la información atribuye a la persona un conocimiento y, por tanto, facilita un control sobre sus datos personales sometidos a tratamiento, de manera que pueda, en su caso, prestar el consentimiento y ejercitar sus derechos.

No se puede ejercer el derecho fundamental a la protección de los datos personales, entendido como el derecho al control sobre la propia información personal, si se desconoce cuáles son las finalidades que justifican el tratamiento de la información personal, quién es el responsable ante el cual se pueden ejercitar los derechos y cuáles son las finalidades que justifican el tratamiento de la información personal, quién es el responsable ante el cual se pueden ejercitar los derechos y cuáles son los posibles cesionarios.

De hecho, el consentimiento del interesado es definido[237] como toda manifestación de voluntad no solo libre, inequívoca y específica, sino también informada. El cumplimiento del principio de información no solo permite el consentimiento, sino también facilita el ejercicio del derecho de acceso, rectificación, cancelación y oposición, incluyendo la posibilidad de ejercitar estos derechos, así como la identidad y dirección del responsable.

---

[236] La LOPD reconoce el derecho a la información por parte del interesado en el momento en que se le soliciten los datos. Lo hace en su artículo 5 los siguientes términos «1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco: a) De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información. b) Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas. c) De las consecuencias de la obtención de los datos o de la negativa a suministrarlos. d) De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición. e) De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento».

[237] Véase el artículo 3. h) LOPD

Como es lógico, si se van a utilizar los datos para una finalidad distinta, hay que volver a informar. Estas características son las que me llevan a afirmar que nos encontramos ante una garantía esencial del derecho fundamental a la protección de datos.

Es importante garantizar el principio de información al interesado, sobre todo cuando existe una situación de desigualdad entre las partes de la relación, o cuando se procede al tratamiento de datos especialmente protegidos. El derecho de información en la recogida de los datos no solo permite al ciudadano un control sobre su información personal, sino que materializa que, aún dentro de una situación de debilidad social, es un sujeto titular de derechos.

Es importante también el cumplimiento del principio de información en el ámbito de las Administraciones Públicas, ya que éstas llevan a cabo tratamientos de datos personales sin consentimiento del interesado, dándose una situación de desigualdad. De esta forma, la ausencia del consentimiento del interesado obliga a reforzar el resto de principio de protección de datos, sobre todo, el principio de información y el de calidad. No parece que existan supuestos claros que justifiquen la excepción del principio de información en el ámbito de las Administraciones Públicas.

Cuando la Administración desarrolle cualquier actividad que suponga un tratamiento de datos personales, aunque sea de cumplimiento obligatorio, incluido el tratamiento desarrollado en virtud de un procedimiento sancionador, está obligada a informar expresamente al ciudadano de lo establecido en el artículo 5 LOPD. La excepción al principio de información al afectado solo es legítima cuando afecte «a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales»[238], supuestos

---

[238] El texto del artículo 24, tras la Sentencia del TC 292/2000, de 30 de noviembre, por la que se declara la inconstitucionalidad y nulidad de los incisos destacados del apartado 1 y todo el apartado 2, establece expresamente: Artículo 24. Otras excepciones a los derechos de los afectados. «1. Lo dispuesto en los apartados 1 y 2 del artículo 5 no será aplicable a la recogida de datos cuando la información al afectado impida o dificulte gravemente el cumplimiento de las funciones de control y verificación de las Administraciones públicas o cuando afecte a la Defensa Nacional, a la seguridad pública o a la persecución de infracciones penales o administrativas.» Esto se aplica a los ficheros

que también justificaban la excepción del derecho de acceso del apartado primero del artículo 23[239] LOPD, y que se encuentran recogidos en el apartado b) del artículo 105[240] CE.

---

policiales de las Fuerzas y Cuerpos de Seguridad, pero no a aquellos con fines administrativos y que están sujetos al régimen general de la LOPD. Por otro lado, el Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, también justificaba en la letra a) del segundo apartado de su artículo 9, la omisión del principio de información cuando era necesario para la protección de la seguridad del Estado, de la seguridad pública o la represión de infracciones penales «Artículo 9. Excepción y restricciones 2. Será posible una excepción en las disposiciones de los artículos 5, 6 y 8 del presente Convenio cuando tal excepción, prevista por la ley de la Parte, constituya una medida necesaria en una sociedad democrática: a) Para la protección de la seguridad del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales». De igual modo, la Directiva 95/46/CE señala en su artículo 13 como excepciones al principio de información, la salvaguardia de la seguridad del Estado, la defensa, la seguridad pública, la persecución de infracciones penales y la protección del interesado o de los derechos y libertades de otras personas «Artículo 13 Excepciones y limitaciones 1. Los Estados miembros podrán adoptar medidas legales para limitar el alcance de las obligaciones y los derechos previstos en el apartado 1 del artículo 6, en el artículo 10, en el apartado 1 del artículo 11, y en los artículos 12 y 21 cuando tal limitación constituya una medida necesaria para la salvaguardia de: a) la seguridad del Estado; b) la defensa; c) la seguridad pública; d) la prevención, la investigación, la detección y la represión de infracciones penales o de las infracciones de la deontología en las profesiones reglamentadas; e) un interés económico y financiero importante de un Estado miembro o de la Unión Europea, incluidos los asuntos monetarios, presupuestarios y fiscales; f) una función de control, de inspección o reglamentaria relacionada, aunque sólo sea ocasionalmente, con el ejercicio de la autoridad pública en los casos a que hacen referencia las letras c), d) y e); g) la protección del interesado o de los derechos y libertades de otras personas. 2. Sin perjuicio de las garantías legales apropiadas, que excluyen, en particular, que los datos puedan ser utilizados en relación con medidas o decisiones relativas a personas concretas, los Estados miembros podrán, en los casos en que manifiestamente no exista ningún riesgo de atentado contra la intimidad del interesado, limitar mediante una disposición legal los derechos contemplados en el artículo 12 cuando los datos se vayan a tratar exclusivamente con fines de investigación científica o se guarden en forma de archivos de carácter personal durante un período que no supere el tiempo necesario para la exclusiva finalidad de la elaboración de estadísticas.

[239] Artículo 23. Excepciones a los derechos de acceso, rectificación y cancelación. «1. Los responsables de los ficheros que contengan los datos a que se refieren los apartados 2, 3 y 4 del artículo anterior podrán denegar el acceso, la rectificación o cancelación en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando».

[240] Artículo 105 «La ley regulará: b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas».

Así, el principio de información forma parte del contenido esencial del derecho fundamental a la protección de datos personales, como ha señalado el Tribunal Constitucional en la Sentencia 292/2000[241], de 30 de noviembre. De hecho, la omisión del principio de información en la recogida de datos puede conllevar la nulidad de pleno derecho del acto administrativo por lesionar derechos y libertades susceptibles de amparo constitucional[242].

El apartado cuarto del artículo 5 LOPD establece:

> *«Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo».*

Por su parte, el RLOPD, expresamente declaraba en el artículo 18.1 que el deber de información «deberá llevarse a cabo a través de un medio que permita acreditar su cumplimiento, debiendo conservarse mientras persista el tratamiento de los datos del afectado». Sin embargo, ya vimos con anterioridad en el Capítulo III de este trabajo, que el Fundamento Jurídico 9 de la Sentencia del Tribunal Supremo, de 15 de julio del 2010, anuló anulado este precepto del Reglamento, al interpretar que no solo obligaba a acreditar el cumplimiento de su deber de informar, sino que exigía que esta acreditación constase documentalmente o en medios informáticos o

---

[241] El Fundamento Jurídico 13 de la STC 292/2000 declara expresamente que «sin la garantía que supone el derecho a una información apropiada mediante el cumplimiento de determinados requisitos legales (art. 5 LOPD) quedaría sin duda frustrado el derecho del interesado a controlar y disponer de sus datos personales, pues es claro que le impedirían ejercer otras facultades que se integran en el contenido del derecho fundamental al que estamos haciendo referencia».

[242] Véase el apartado primero del artículo 48 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. Artículo 48. Anulabilidad. «1. Son anulables los actos de la Administración que incurran en cualquier infracción del ordenamiento jurídico, incluso la desviación de poder».

telemáticos, lo que podía ser una recomendación, pero no una obligación adicional al no estar establecida en la LOPD, que dejaba libertad de forma, tanto para informar como para acreditar el cumplimiento de dicho deber, contraviniendo así la Ley.

En otro orden de cosas, se debe hacer mención al hecho de que el derecho de información en la recogida de los datos incluye una información expresa, precisa e inequívoca en relación con los destinatarios de la información. No es posible ejercer el control sobre la propia información personal si no se conocen los posibles cesionarios. No obstante, son muchas las posibles cesiones de datos personales que conoce el responsable del fichero ya desde el momento de la recogida de los datos. Afirma TRONCOSO REIGADA que la incorporación de todas ellas a la leyenda informativa haría de ésta un texto poco comprensible, dificultando el cumplimiento de la finalidad del propio principio de información. Por ello, no es razonable la inclusión en la leyenda informativa de una enumeración exhaustiva de todas las cesiones previstas en la legislación, sino únicamente de algunas de ellas. Es aconsejable la inclusión de las cesiones que se realicen con carácter periódico, las realizadas a otras Administraciones Públicas para el ejercicio de competencias semejantes y las previstas en la legislación específica. En cambio, no es recomendable la inclusión de las cesiones que se encuentran expresamente previstas en la LOPD. Tampoco deben ser incluidas las cesiones necesarias para la tramitación de procedimientos administrativos[243].

Igualmente, el artículo 27[244] LOPD obliga al responsable, en el momento en que efectúe la primera cesión, a informar a los afectados, indicando la

---

[243] Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant Lo Blanch, pp 459-460.

[244] Expresamente reconoce el artículo 27 LOPD en relación al derecho de acceso que: «1. El derecho de acceso es el derecho del afectado a obtener información sobre si sus propios datos de carácter personal están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de los mismos. 2. En virtud del derecho de acceso el afectado podrá obtener del responsable del tratamiento información relativa a datos concretos, a datos incluidos en un determinado fichero, o a la totalidad de sus datos sometidos a tratamiento. No obstante, cuando

finalidad del fichero, la naturaleza de los datos cedidos y el nombre y la dirección del cesionario, salvo que: i) la comunicación venga impuesta por una ley; ii) responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros; iii) tenga por destinatario a los órganos judiciales, Ministerio Fiscal, Defensor del Pueblo o Tribunal de Cuentas, en el ejercicio de las funciones que tenga atribuidas; o iv) se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

Por último, ya hemos visto anteriormente que la LOPD obliga a informar de forma expresa, precisa e inequívoca cuando los datos de carácter personal no hayan sido recabados del interesado. No obstante, existe la posibilidad de exoneración de este deber en los supuestos recogidos en el apartado quinto del artículo 5. Así,

> *«No será de aplicación lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias».*

---

razones de especial complejidad lo justifiquen, el responsable del fichero podrá solicitar del afectado la especificación de los ficheros respecto de los cuales quiera ejercitar el derecho de acceso, a cuyo efecto deberá facilitarle una relación de todos ellos. 3. El derecho de acceso es independiente del que otorgan a los afectados las leyes especiales y en particular la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común».

1.2 El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico

Se ha declarado en el apartado anterior que el consentimiento del interesado es un principio fundamental de la protección de datos personales, que se aplica tanto para el tratamiento de datos personales, recogido en el artículo 6 LOPD, como para la comunicación de datos a un tercero, establecida en el artículo 11 LOPD.

El consentimiento del afectado se encuentra definido en la letra h) del artículo 3 LOPD como «toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen». No obstante, los ficheros de titularidad pública de las Administraciones Públicas disponen de una regulación específica que afecta al principio del consentimiento del afectado.

La LOPD señala en el artículo 6.2[245] que no será preciso el consentimiento para el tratamiento «cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias».

La mayoría de los tratamientos de datos personales que realizan las Administraciones se produce sin consentimiento del interesado porque los datos se recogen para el ejercicio de las funciones propias de las

[245] En relación con el consentimiento del afectado, el artículo 6.2 LOPD declara que «no será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado».

Administraciones Públicas en el ámbito de sus competencias. Afirman ANDREU MARTÍNEZ y PLANA ARNALDOS que es lógica esta excepción, ya que el cumplimiento de funciones administrativas y de potestades de derecho público –que requiere el tratamiento de datos personales– no puede supeditarse a la existencia de un consentimiento del interesado. Además, estos tratamientos no solo se encuentran exceptuados del consentimiento por el ejercicio de funciones propias de las Administraciones Públicas en el ámbito de sus competencias, sino también en virtud de una habilitación legal, que, si bien no siempre prevé el tratamiento de datos personales, sí regula el cumplimiento de una función administrativa, que requiere, para su desarrollo, el tratamiento de datos personales[246].

La LOPD también establece como excepción al consentimiento cuando al tratamiento se refiere a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y es necesario para su mantenimiento y cumplimiento. Esta excepción de consentimiento se aplica en muchas ocasiones a los responsables de ficheros privados. Sin embargo, ésta es también una excepción que se utiliza en el ámbito de la Administración Pública. Lógicamente, el hecho de que la ley disponga de forma expresa la necesidad de llevar a cabo un tratamiento de datos personales, también supone una excepción del consentimiento del interesado[247]. El legislador no solo ha intervenido para regular determinadas actividades y funciones, que tendría de esta forma una cobertura legal, sino para establecer expresamente la necesidad de un tratamiento de datos personales sin consentimiento del interesado.

---

[246] Andreu Martínez, M. B. y Plana Arnaldos, M. C. (2013). El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica.* Navarra: Aranzadi, pp 133-134.

[247] Al referirse al consentimiento del afectado, el artículo 6.1 LOPD expresamente expone que «el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa».

No obstante, si bien en muchos supuestos los tratamientos de datos personales que efectúan las Administraciones Públicas están exceptuados del consentimiento del interesado por desarrollarse para el ejercicio de funciones administrativas en el ámbito de sus competencias, por referirse a las partes de una relación negocial o administrativa o por existir una habilitación legal, en ocasiones es conveniente solicitar el consentimiento del interesado, especialmente cuando se prestan servicios públicos por voluntad del interesado o de las personas que ostentan su representación legal.

Tanto la presencia de excepciones al consentimiento del interesado para el tratamiento como el propio consentimiento de éste, no puede justificar el incumplimiento de otros principios de protección de datos personales. Esto es muy importante en relación con el principio de calidad. Así, por ejemplo, el consentimiento del interesado no convalida un tratamiento de datos personales excesivos que va más allá de la finalidad. Además, en muchas ocasiones, no existe un consentimiento libre, tal y como exige y tipifica la letra h) del artículo 3 LOPD.

Generalmente se considera que el pilar básico en materia de protección de datos personales lo constituye el consentimiento del titular de los datos. Es éste el que legitima el tratamiento de datos, y el que permite que el titular tenga un cierto poder de control sobre el uso que se le da a sus datos personales[248]. Así se dispone en el primer apartado del artículo 6 LOPD al afirmar que

> *«…el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa»*

[248] Véase la Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre, FJ 6º ya comentado con anterioridad.

En el artículo 6.2 LOPD se establecen las excepciones a esta regla general, esto es, los supuestos en que pueden tratarse los datos sin contar con dicho consentimiento.

Ahora bien, el artículo 7 de la Directiva 95/46/CE recoge el consentimiento del afectado, dentro del listado de supuestos en que los Estados miembros pueden permitir el tratamiento de los datos. Los restantes supuestos de este artículo constituyen para la legislación española excepciones a la necesidad de contar con el consentimiento del interesado[249].

El consentimiento tiene una importancia evidente como elemento configurador del derecho fundamental a la protección de datos personales[250], sin embargo, en la práctica la importancia de éste, no es tan decisiva como a primera vista pudiera parecer.

1.3 El consentimiento del interesado

1.3.1 Diferencia entre el RGPD y la legislación nacional LOPD y RLOPD

Anteriormente se ha expuesto que el consentimiento aparece definido en el apartado 11 del artículo 4 del RGPD en los siguientes términos:

---

[249] El Grupo del Artículo 29, en su Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011, WP187, señala que «algunos Estados miembros lo consideran un fundamento preferente, en ocasiones parecido a un principio constitucional, vinculado al sistema de protección de datos como derecho fundamental. Otros Estados miembros lo consideran una de las seis opciones, un requisito operativo que no es más importantes que las otras opciones. […] El orden en que se citan los fundamentos jurídicos en el artículo 7 es pertinente, pero no significa que el consentimiento sea siempre el fundamento más adecuado para legitimar el tratamiento de datos personales». A su vez, el apartado segundo del artículo 8 de la Carta de Derechos Fundamentales de la Unión Europea (DOCE C 364 18/12/2000), reconoce que los datos se tratarán sobre la base del consentimiento de la persona afectada, o en virtud de otro fundamento legítimo previsto por la ley.

[250] Sobre el concepto del derecho fundamental a la protección de datos y su consolidación, ver Murillo de la Cueva, P. L. (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos; Martínez Martínez, R. (2004), Una aproximación crítica a la autodeterminación informativa, Madrid: Civitas-APDCM.

> *«…toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».*

A nivel interno, el consentimiento del interesado aparece definido por el apartado h) del articulo 3 de la LOPD y por la letra d) del artículo 5.1 del RLOPD. En ambos instrumentos normativos la definición coincide:

> *«…toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen».*

Podemos comprobar las diferencias existentes entre ambas definiciones. Además del cambio de *consentir* por *aceptar*, la novedad es que se especifican dos formas de expresar el consentimiento: i) mediante una declaración; y, ii) mediante una acción. Por tanto, no cabe el llamado consentimiento tácito.

1.3.2 El Considerando 32 del RGPD

En relación al consentimiento, el RGPD estipula en su Considerando 32

> *«El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el*

consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta».

Luego queda claro que el silencio o la inacción, no pueden considerarse como una declaración de consentimiento, sino que tienen que ser un acto afirmativo claro y para unos fines específicos.

Ahora bien, como sabemos, la Directiva 95/46/CE es derogada[251] por el RGPD con efecto a partir del 25 de mayo de 2018. El Considerando 171 de éste nos facilita las claves de qué hacer con los tratamientos de datos iniciados antes del 25 de mayo de 2018, y que se basen en un consentimiento que cumpla los requisitos de la antigua Directiva, y nuestra LOPD.

«La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento. Las decisiones de la Comisión y las autorizaciones de las autoridades de control basadas en la Directiva 95/46/CE permanecen en vigor hasta que sean modificadas, sustituidas o derogadas».

Podemos distinguir los siguientes supuestos de tratamiento de datos:

---

[251] En relación a la derogación de la Directiva 95/46/CE, el artículo 94 RGPD manifiesta que «queda derogada la Directiva 95/46/CE con efecto a partir del 25 de mayo de 2018».

Tratamientos de datos iniciados antes del 25 de mayo de 2018, basados en un consentimiento que sí cumple los requisitos del RGPD. No es necesario pedir al interesado ni que éste dé su consentimiento de nuevo, si los datos se van a seguir tratando para los mismos fines que el interesado consintió. Bastaría una comunicación de la modificación normativa.
Tratamientos de datos iniciados antes del 25 de mayo de 2018, basados en un consentimiento que sí cumple con los requisitos del RGPD. Sí es necesario pedir al interesado y que éste dé su consentimiento de nuevo, si los datos se van a tratar para fines distintos de los que el interesado consistió. Habría que aprovechar esta petición para informar de las nuevas condiciones.
Tratamiento de datos iniciado antes del 25 de mayo de 2018, basados en un consentimiento que no cumple los requisitos del RGPD, en especial, aquellos que se basan en un consentimiento tácito. Deben ajustarse a los requisitos del RGPD antes de esa fecha, y sí es necesario pedir al interesado que dé su consentimiento expreso.

1.3.3 Diferencias entre el RGPD y la Directiva 95/46/CE

Por su parte, la Directiva 95/46/CE tipifica el consentimiento del interesado en el apartado h de su artículo 2. Los términos literales son:

> *«…toda manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan».*

La modificación más importante que ha supuesto la definición del RGPD, es haber introducido el término *inequívoco* como uno de los requisitos de la «indicación de los deseos del sujeto de los datos» (o de la «manifestación de voluntad del interesado»), para que sea válido el consentimiento.

Sin embargo, este requisito ya estaba incluido en el apartado a) del artículo 7[252] de la Directiva, así como en el apartado h) del artículo 3 de nuestra LOPD. Luego no supone una novedad el texto del nuevo RGPD.

1.3.4 La configuración del consentimiento en el RGPD

Ya hemos visto que el consentimiento es una declaración de voluntad procedente del sujeto titular de los datos personales por la que éste acepta que los mismos se sometan a tratamiento. En la legislación interna, y siguiendo a lo recogido en la Directiva 95/46/CE[253], tanto la letra h) del artículo 3 LOPD, como la letra d) del apartado primero del artículo 5 RLOPD, lo caracterizan como una declaración de voluntad «libre, inequívoca, específica e informada».

El artículo 6 RGPD mantiene, a propósito de la licitud en el tratamiento de datos personales, los mismos supuestos de legitimación del tratamiento recogidos en el artículo 7 de la Directiva 95/46/CE, con alguna matización. Así, el artículo 6 RGPD afirma que «el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones», y la letra a) de su artículo 6.1 declara como condición que «el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos».

Por otra parte, el consentimiento del interesado es definido en dicho texto legal por el apartado 11 del artículo 4 como:

> *«toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen».*

---

[252] «Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca».

[253] Conforme a lo dispuesto de la Directiva 95/46/CE en sus apartados correspondiente a la letra h) del artículo 2 y la letra a) del artículo 7

La referencia a un consentimiento específico implica que deben determinarse en el momento de la recogida de los fines concretos para los cuales se recaban los datos, que deben ser explícitos y legítimos, aunándose así los principios de licitud del tratamiento y finalidad. Por tanto, no es admisible un consentimiento indiscriminado, sin delimitación de los fines o actividades para los cuales se recaba.

Así se establece en la letra a) del artículo 6.1 RGPD, cuando señala, a propósito de la licitud del tratamiento, que el interesado debe haber prestado su consentimiento «para uno o varios fines específicos». Además, el apartado b) del artículo 5 RGPD, incluye dentro de los principios relativos al tratamiento de datos personales el de finalidad, al señalar que los datos deberán ser «recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines».

Asimismo, la declaración de voluntad del interesado solo puede considerarse correcta cuando se forma de manera consciente, racional y libre. Solo será válida, y producirá plenos efectos, la voluntad consciente y libremente declarada. En caso contrario, habrá de considerar viciado el consentimiento[254]. Para garantizar la validez del consentimiento se requiere que sea «informado» y «libre».

El requisito relativo a que el consentimiento sea informado, conlleva una vinculación de dos principios básicos en materia de protección de datos. Me refiero a los principios de licitud y transparencia[255]. La exigencia de un consentimiento informado permite que el interesado conozca con anterioridad a la prestación del consentimiento que sus datos van a ser

---

[254] Véase Delgado Echevarría, J. (2005). La voluntad negocial y sus vicios. En Lacruz Berdejo, J. L. y otros. *Elementos de Derecho civil, Tomo I. Parte General. Volumen III*. Madrid: Dykinson, pp. 153 y ss.

[255] Por lo que respecta a los principios relativos al tratamiento, expresamente estipula el apartado a) del artículo 5.1 RGPD que «los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)».

objeto de tratamiento, los fines, la identidad del responsable y demás circunstancias señaladas en la normativa.

Ahora bien, en la actualidad, la complejidad de las prácticas de recolección de datos, en especial en el ámbito de internet, y los modelos comerciales utilizados, hacen que difícilmente una persona pueda ser consciente y controlar la información que está compartiendo[256].

De ahí que el RGPD tenga como uno de sus objetivos principales reforzar la transparencia y el derecho a la información, de manera que los ciudadanos tengan un conocimiento pleno de quién trata sus datos, de qué manera, con qué fines, durante cuánto tiempo, o de los derechos de que dispone. Con ello se pretende reforzar el control del titular sobre sus datos personales.

En este sentido, el artículo 12 RGPD regula la transparencia de la información y la comunicación. En él se establecen los requisitos que debe cumplir la información dirigida al público o al interesado. Así, el responsable del tratamiento facilitará al interesado la información «en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo». Esto es sumamente importante en el entorno en línea, en donde el acceso a las políticas de privacidad, en la mayoría de las ocasiones son difíciles de localizar, y poco comprensibles[257].

Por otra parte, el consentimiento ha de prestarse de manera libre. El Considerando 43 declara expresamente:

---

[256] Entender, y tener siempre presente esta idea, me parece crucial. No debemos cejar hasta encontrar una solución al respecto.

[257] El Grupo del Artículo 29, en su Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011, WP187, señala los requisitos que se deben cumplir para garantizar una información adecuada: «i) Calidad de la información – la manera en que se presenta la información (texto claro, sin jerga, comprensible, visible) es esencial para determinar si el consentimiento es manifestación de voluntad «informada». La forma en que se suministra esta información depende del contexto: el usuario medio/habitual debe ser capaz de entenderla; y ii) Accesibilidad y visibilidad de la información – La información debe comunicarse directamente a las personas. No basta con que la información esté «disponible» en algún lugar. La información debe ser claramente visible (tipo y tamaño de los caracteres), destacada y completa.

«Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento, en particular cuando dicho responsable sea una autoridad pública y sea por lo tanto improbable que el consentimiento se haya dado libremente en todas las circunstancias de dicha situación particular. Se presume que consentimiento no se ha dado libremente cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aun cuando este no sea necesario para dicho cumplimiento».

Esta previsión se venía reclamando o manifestando con antelación. El Grupo del Artículo 29 hizo mención a ella desde el año 2001[258].

---

[258] Véase el Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral, de 13 de septiembre de 2001 WP48 «The Article 29 Working Party takes the view that where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice. An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut where, as is often the case, all employers impose the same or a similar condition of employment.»; The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, de 01 de diciembre de 2009 WP168 «66. There are many cases in which consent can not be given freely, especially when there is a clear unbalance between the data subject and the data controller (for example in the employment context or when personal data must be provided to public authorities); y por último, el Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011 WP187 «El consentimiento únicamente puede ser válido si el interesado puede elegir una opción real y no hay ningún riesgo de engaño, intimidación, coerción o consecuencias negativas significativas en caso de que no consienta. Si las consecuencias del consentimiento socavan la libertad de elección de la persona, el consentimiento no es libre. La propia Directiva prevé en su artículo 8, apartado 2, letra a), que, en algunos casos, a determinar por los Estados miembros, la prohibición del tratamiento de categorías especiales de datos personales no puede ser suprimida por el consentimiento del interesado. Un ejemplo de lo anterior es

Ahora bien, se ha de destacar que en la propuesta del RGPD de fecha 25 de enero de 2012[259] se detallaba en el apartado cuarto del artículo 7 que:

> *«El consentimiento no constituirá una base jurídica válida para el tratamiento cuando exista un desequilibro claro entre la posición del interesado y el responsable del tratamiento».*

De igual forma, en los Considerandos 33[260] y 34[261] de la propuesta, se remarcaba que, para garantizar el consentimiento libre, éste no puede constituir una base jurídica válida cuando la persona no goza de verdadera libertad de elección y no está, por tanto, en condiciones de denegar o retirar su consentimiento sin sufrir perjuicio alguno. El consentimiento no debe

---

el caso del interesado que está bajo la influencia del responsable del tratamiento, como sucede en la relación laboral. En este ejemplo, aunque no necesariamente en todos los casos, el interesado puede estar en una situación de dependencia del responsable del tratamiento debido a la naturaleza de la relación o a circunstancias particulares, y puede temer recibir un trato diferente si no da su consentimiento para el tratamiento de los datos». En idéntico sentido se manifiesta el Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), de 15 de febrero de 2007 WP131 y el Segundo dictamen 4/2009 sobre la Norma internacional para la protección de la intimidad y los datos personales de la Agencia Mundial Antidopaje (AMA), sobre disposiciones relacionadas del Código AMA y sobre otros aspectos relacionados con la intimidad en el contexto de la lucha contra el dopaje en el deporte por parte de la AMA y de las organizaciones nacionales antidopaje, de 06 de abril de 2009 WP 162.

[259] Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), de 25 de enero de 2012 COM(2012) 11 final http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_es.pdf

[260] En el Considerando 33 de la Propuesta RGPD se declaraba expresamente que «con el fin de garantizar el consentimiento libre, debe aclararse que este no constituye un fundamento jurídico válido cuando la persona no goza de verdadera libertad de elección y por tanto no está en condiciones de denegar o retirar su consentimiento sin sufrir perjuicio alguno».

[261] En el Considerando 34 de la Propuesta RGPD se reconoce que «el consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando exista un desequilibro claro entre el interesado y el responsable del tratamiento. Así sucede especialmente cuando el primero se encuentra en una situación de dependencia respecto del segundo, por ejemplo, cuando los datos personales de los trabajadores son tratados por el empresario en el contexto laboral. Cuando el responsable del tratamiento sea una autoridad pública, solo habría desequilibrio en las operaciones específicas de tratamiento de datos en las que la autoridad pública puede imponer una obligación en virtud de sus poderes públicos correspondientes, sin que pueda considerarse el consentimiento libremente dado, teniendo en cuenta el interés del interesado».

constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal cuando «exista un desequilibrio claro entre el interesado y el responsable del tratamiento».

Como se ha comprobado, dichas indicaciones no se han trasladado tal cual en la redacción final del RGPD. Ahora bien, dicha eliminación no implica que el consentimiento sea por ello válido en las situaciones que preveía dicho precepto. El requisito de que el consentimiento se preste de forma libre sigue existiendo. Por ello, en aquellos casos en los que el interesado no tenga una verdadera libertad de elección, su consentimiento estará viciado y no podrá legitimar el tratamiento de datos personales. Si bien es cierto que, el hecho de que la referencia explícita al desequilibrio entre las partes se elimine del texto, y se reserve para el considerando 43, conlleva una cierta reducción de su virtualidad y, sobre todo, de su aplicación generalizada.

El artículo 7.2 pretende aclarar cuándo debe considerarse válido el consentimiento para el tratamiento de datos personales cuando éste sea dado en el contexto de una declaración escrita que también se refiera a otros asuntos. De este modo, el consentimiento deberá solicitarse de tal forma que se distinga de ese otro asunto. Con ello, se pretende establecer garantías para asegurar que el interesado es consciente de que está prestando su consentimiento y en qué medida lo hace. Esta previsión se encuentra ligada a la especificidad del consentimiento, y debe implicar dos cosas:

1) Evita que el consentimiento otorgado para un asunto pueda utilizarse como base para tratar datos personales para otro distinto[262].

---

[262] El Grupo del Artículo 29, en su Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011, WP187, pone como ejemplo las redes sociales. De este modo, «el acceso a los servicios de redes sociales suele estar sujeto a la autorización de diferentes tipos de tratamiento de datos personales. Al usuario se le puede pedir su consentimiento para recibir publicidad comportamental para inscribirse en un servicio de red social, sin más especificaciones ni opciones alternativas. Considerando la importancia que han adquirido algunas redes sociales, ciertas categorías de usuarios (como los adolescentes) aceptarán la recepción de publicidad comportamental para evitar el riesgo de ser parcialmente excluidos de las interacciones sociales. El usuario debería estar en condiciones de dar su consentimiento libre y específico para recibir la publicidad comportamental, independientemente de su acceso al servicio de la red social. Para ofrecer al usuario esta posibilidad

Debe permitir al interesado como regla general, y en consonancia con el requisito de libertad del consentimiento, prestarlo para uno de los asuntos y negarlo para tratar los datos para otro distinto[263].

1.4 Licitud del tratamiento y condiciones del consentimiento

1.4.1 Circunstancias en las que no es necesario el consentimiento

Se ha afirmado anteriormente que el artículo 6 de la LOPD recoge expresamente que:

> *«1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. 2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el*

---

podría utilizarse una ventana desplegable. […] El cará ter específico del consentimiento también significa que, si los fines para los que los datos son tratados por el responsable cambian en algún momento, el usuario deberá ser informado y estar en condiciones de dar su consentimiento para el nuevo tratamiento de datos. La información que se facilite deberá mencionar las consecuencias del rechazo de los cambios propuestos».

[263] A nivel interno, el artículo 15 del RLOPD se refiere a la solicitud del consentimiento en el marco de una relación contractual para fines no relacionados directamente con la misma en los siguientes términos: «Si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos».

del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado».

Igualmente, el RGPD establece la licitud del tratamiento en su artículo 6:

« 1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones».

En relación a las condiciones del consentimiento, el RGPD especifica que el tratamiento de los datos solo será lícito si el interesado dio su consentimiento para uno o varios fines específicos, mientras que la LOPD solo habla de un consentimiento inequívoco del afectado.

En cuanto a las diferencias entre la LOPD y el nuevo RGPD sobre los casos en los que no se requiere el consentimiento del afectado o interesado para el tratamiento de sus datos, la norma europea añade tres nuevos supuestos, respecto de la LOPD:

1) El tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

El tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; y,

El tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

Por lo que se refiere al apartado f) del artículo 6.1 RGPD, el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, en el RGPD no figura el requisito que exige la LOPD de que «los datos figuren en fuentes accesibles al público», por lo que se entiende que, al ser de aplicación directa, ya no sería necesario dicho requisito.

La coletilla final de este apartado f) del artículo 6.1 del RGPD tiene una redacción diferente a la de nuestra LOPD. En ésta, se dice: «siempre que no se vulneren los derechos y libertades fundamentales del interesado», mientras que en el RGPD se dice: «siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales en particular cuando el interesado sea un niño».

La redacción del RGPD es más abierta, en la misma línea del artículo 10.2.a) del RLOPD, pues se pueden dar conflictos entre dos bienes jurídicos protegidos sin que se produzca la vulneración de uno de ellos.

1.4.2 Condiciones del consentimiento

Aunque el artículo 7 del RGPD se titula «Condiciones para el consentimiento», realmente éstas ya se han enumerado en la definición del artículo 4, a las que desde aquí nos remitimos.

El único apartado del artículo 7 que se refiere a una de esas condiciones básicas del consentimiento, la libertad, es el apartado 4, en el que se ofrece criterios para determinar si el consentimiento ha sido realmente libre o se ha impuesto al usuario el tratamiento de datos que no son necesarios para la

prestación de un servicio, como condición necesaria para beneficiarse del mismo.

1.4.3 Prueba del consentimiento

Los apartados 1 y 2 del artículo 7 del RGPD no se refieren tanto a unas condiciones del consentimiento, sino a la prueba de que éste se dio y que se dio cumpliendo las condiciones esenciales que debe tener para que sea válido:

> *«1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. 2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento».*

Nuestra LOPD solo exige el consentimiento expreso y por escrito del afectado en el caso de tratamiento de datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias[264].

Por lo demás, la forma de recabar, y de obtener tácitamente, el consentimiento del interesado, prevista en el artículo 14[265] del RLOPD

---

[264] Por lo que se refiere a los datos especialmente protegidos, expresamente se recoge en el artículo 7.2 LOPD que «solo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado».

[265] Conforme al artículo 14 RLOPD: «1. El responsable del tratamiento podrá solicitar el consentimiento del interesado a través del procedimiento establecido en este artículo, salvo cuando la

desarrollo dela LOPD, ya no tiene validez, pues el RGPD exige que el consentimiento sea siempre expreso.

1.5 Formas de prestar el consentimiento

La normativa europea no prevé requisitos específicos sobre la forma en la que debe prestarse el consentimiento. Por razones de flexibilidad, el texto definitivo de la Directiva 95/46/CE desechó la referencia a la necesidad de un consentimiento escrito.

De esta manera, puede entenderse que se ha prestado el consentimiento cuando exista un signo que claramente revele la voluntad del sujeto de aceptar el tratamiento de datos, ya sea por escrito, verbalmente o a través de un comportamiento del que pueda razonablemente deducirse dicho consentimiento.

Por ello, el artículo 7 de la Directiva 95/46/CE establece como primer supuesto de legitimación del tratamiento, el que el interesado haya prestado

---

Ley exija al mismo la obtención del consentimiento expreso para el tratamiento de los datos. 2. El responsable podrá dirigirse al afectado, informándole en los términos previstos en los artículos 5 de la Ley Orgánica 15/1999, de 13 de diciembre y 12.2 de este reglamento y deberá concederle un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal. En particular, cuando se trate de responsables que presten al afectado un servicio que genere información periódica o reiterada, o facturación periódica, la comunicación podrá llevarse a cabo de forma conjunta a esta información o a la facturación del servicio prestado, siempre que se realice de forma claramente visible. 3. En todo caso, será necesario que el responsable del tratamiento pueda conocer si la comunicación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado. 4. Deberá facilitarse al interesado un medio sencillo y gratuito para manifestar su negativa al tratamiento de los datos. En particular, se considerará ajustado al presente reglamento los procedimientos en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento, la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido. 5. Cuando se solicite el consentimiento del interesado a través del procedimiento establecido en este artículo, no será posible solicitarlo nuevamente respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año a contar de la fecha de la anterior solicitud».

su consentimiento de forma «inequívoca»[266]. Al hilo de esta redacción, tanto la LOPD como el RLOPD recogen el carácter «inequívoco» del consentimiento[267]. Sin embargo, para cierto tipo de datos, como son los datos sensibles, se sustituye el consentimiento inequívoco por un consentimiento expreso, e incluso otorgado en forma escrita en ciertos supuestos[268]. Ahora bien, más allá de estos supuestos, la regla general es la del consentimiento inequívoco.

Señalan ANDREU MARTÍNEZ Y PLANA ARNALDOS que para que el consentimiento pueda considerarse inequívoco, es necesario que el procedimiento para recabarlo y prestarlo no deje lugar a dudas sobre la intención del sujeto al respecto. Dentro de este consentimiento inequívoco se entiende incluido el consentimiento implícito o tácito, entendiendo por tal el que puede deducirse de una actuación u omisión que presupone la existencia de tal consentimiento[269]. Se admite así que el silencio pueda considerarse como consentimiento al tratamiento de datos personales[270].

Siguiendo este criterio, el RLOPD establece en el apartado segundo de su artículo 14 un mecanismo para recabar el consentimiento, que permite que

---

[266] Así, el artículo 7 de la Directiva 95/46/CE establece que «los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca».

[267] Véase el apartado h) del artículo 3 LOPD, y la letra d) del artículo 5.1 RLOPD.

[268] Véase el artículo 7 LOPD referente a los «datos especialmente protegidos» que transpone el artículo 8 de la Directiva 95/46/CE.

[269] Entre otros, Fernández López, J. M. (2010). Principio de consentimiento. En Troncoso Reigada, A. (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Civitas, pp. 454 y ss.; Aparicio Salom, J. (2009). Estudios sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Navarra: Aranzadi, pp. 118 y ss.; Guerrero Picó, M.C. (2006). El impacto de internet en el derecho fundamental a la protección de datos de carácter personal. Madrid: Civitas, p. 259.

[270] Andreu Martínez, M. B. y Plana Arnaldos, M. C. (2013). El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica.* Navarra: Aranzadi, p 139.

el responsable pueda dirigirse al interesado, informándole de los extremos previstos en la normativa de protección de datos, y concediéndole «un plazo de treinta días para manifestar su negativa al tratamiento, advirtiéndole de que en caso de no pronunciarse a tal efecto se entenderá que consiente el tratamiento de sus datos de carácter personal».

Uno de los puntos más novedosos y destacados de la Propuesta de RGPD del año 2012, fue la sustitución del término «inequívoco» por el de «explícito». Así, el apartado 8 del artículo 4 definía el consentimiento del interesado como una manifestación de voluntad «explícita», por la que el interesado acepta «ya sea mediante una declaración ya sea mediante una clara acción afirmativa, el tratamiento de datos personales que le conciernen». Con ello, la propuesta dejaba fuera del consentimiento a las omisiones o al silencio[271].

No obstante, la versión definitiva del RGPD mantiene el término «inequívoco» para los tratamientos de datos que no se refieran a las categorías especiales de datos personales del artículo 9.

1.6 Salvaguarda y límites al poder de disposición del titular de los datos.

La regla general para poder proceder al tratamiento de los datos de una persona es que ésta haya consentido, en línea con la consideración de este derecho como fundamental, su conexión con el derecho a la intimidad y, en

[271] Así lo recogía expresamente su Considerando 25, al establecer expresamente que «se debe dar el consentimiento de forma explícita por cualquier medio apropiado que permita la manifestación libre, específica e informada de la voluntad del interesado, ya sea mediante una declaración o una clara acción afirmativa del interesado, que garantice que la persona es consciente de que está dando su consentimiento al tratamiento de datos personales, incluso mediante la selección de una casilla de un sitio web en internet o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio o la inacción no deben constituir consentimiento. El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo fin o fines».

sentido amplio, la dignidad de la persona. Este concepto está vinculado a la idea de que el interesado debe controlar el uso que se hace de sus datos.

El consentimiento es, por tanto, el elemento esencial que, no solo legitima el tratamiento, sino que refleja el poder de disposición del titular sobre sus propios datos. No obstante, como he destacado con anterioridad, en muchas ocasiones, el consentimiento se forma sin la necesaria información y en un entorno de desequilibrio entre las partes, lo que impide considerar que se ha formado de manera «libre», requisito esencial del consentimiento válido.

De este modo, la falta de información real y el desequilibrio entre las partes pone en riesgo[272] el derecho del titular a decidir sobre sus datos. A este respecto, afirman ANDREU MARTÍNEZ y PLANA ARNALDOS que, con carácter general, los mecanismos que ofrece la legislación de protección de datos personales para salvaguardar el derecho a la autodeterminación del titular de los datos son varios: revocación del consentimiento, y ejercicio de los derechos de oposición, rectificación y cancelación. Ahora bien, tales posibilidades, en especial el reconocimiento de los derechos de oposición y cancelación, sin garantizar que previamente existe un consentimiento libremente formado y declarado, se convierten en una carga y no en una garantía para el derecho fundamental a la protección de datos. En la práctica, si la única garantía de control de sus datos por el titular es el derecho de cancelación, o de oposición, la situación sería similar a admitir el tratamiento no consentido con el límite de los derechos de oposición y cancelación, y no es este el sistema articulado en la legislación sobre protección de datos.

La cuestión radica en determinar cómo se ha de configurar por parte del ordenamiento jurídico el consentimiento para que realmente sea éste el

---

[272] El Grupo del Artículo 29, declara en el documento « El futuro de la privacidad: contribución común a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de los datos de carácter personal», 1 de diciembre de 2009, WP 168 que «la complejidad de las prácticas de recogida de datos, modelos empresariales, relaciones con los vendedores y aplicaciones tecnológicas llega en muchos casos a sobrepasar la capacidad o la voluntad de la persona para tomar decisiones de control sobre el uso e intercambio de información por medio de una elección activa».

elemento esencial que legitima el tratamiento de datos. En esta cuestión es importante tener en cuenta no solo la normativa de protección de datos personales, sino también las normas de protección de consumidores y usuarios, en la medida en que sean aplicables[273].

En primer lugar, es necesario que exista posibilidad efectiva de consentir o no, lo cual requiere información y libertad, es decir, que exista efectivamente la opción para consentir o no el tratamiento de los datos. Para ser válido, el consentimiento debe ser «informado». Por otro lado, resulta esencial la forma en la que se presta el consentimiento y cómo se regula este extremo.

La información se configura como requisito para el poder de disposición efectivo y la validez del consentimiento. El artículo 5 LOPD señala cuáles son los requisitos del «consentimiento informado». En primer lugar, la información, cuando se solicite el consentimiento para recabar los datos del titular, ha de ser expresa, precisa e inequívoca, requisitos similares a los del propio consentimiento. En segundo lugar, establece el contenido de la información que se ha de facilitar al interesado[274]. En el mismo sentido, el RGPD, en aras al fortalecimiento de la información y la transparencia, regula la transparencia de la información y la comunicación, estableciendo en su artículo 12 los requisitos que deben cumplir la información, facilitada por escrito o por otros medios, inclusive medios electrónicos, relativa al tratamiento dirigida al interesado que ha de ser concisa, transparente,

---

[273] Andreu Martínez, M. B. y Plana Arnaldos, M. C. (2013). El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica.* Navarra: Aranzadi, pp 145-147.

[274] Conforme al primer apartado del artículo 5 LOPD, los afectados deberán ser informados: i) de la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información; ii) del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas; iii) de las consecuencias de la obtención de los datos o de la negativa a suministrarlos; iv) de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición; y v) de la identidad y dirección del responsable del tratamiento o, en su caso, de su representante. Sin embargo, no será necesario la información referente a los apartados ii), iii) y iv), si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

inteligible, de fácil acceso, con un lenguaje claro y sencillo. Por su parte, los artículos 13 y 14 de dicha norma, establecen el contenido de la información que se ha de suministrar al titular de los datos, cuando los datos se obtengan del propio interesado en el primer supuesto, y en el supuesto del artículo 14, cuando los datos no se hayan obtenido directamente por el interesado.

El consentimiento válido requiere de manera esencial que se forme libremente, lo que exige información suficiente para que se pueda formar la voluntad y permita la decisión consciente del titular. Esto implica tanto el suministro de información suficiente, clara y anticipada, como el cumplimiento del contenido imperativo al que la ley obliga.

1.7 Retirada / Revocación del Consentimiento

En cuanto a la retirada o revocación del consentimiento, hay algunas diferencias en el tratamiento que se hace en el RGPD[275] respecto del que hace nuestra LOPD[276] y el RLOPD[277].

---

[275] Por lo que se refiere a las condiciones para el consentimiento, se recoge en el artículo 7.3 RGPD que «el interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo».

[276] Respecto al consentimiento del afectado, expresamente se declara en el artículo 6.3 LOPD que «el consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos».

[277] En relación a la revocación del consentimiento, el artículo 17 RLOPD afirma que «el afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En particular, se considerará ajustado al presente reglamento el procedimiento en el que tal negativa pueda efectuarse, entre otros, mediante un envío prefranqueado al responsable del tratamiento o la llamada a un número telefónico gratuito o a los servicios de atención al público que el mismo hubiera establecido. No se considerarán conformes a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, los supuestos en que el responsable establezca como medio para que el interesado pueda manifestar su negativa al tratamiento el envío de cartas certificadas o envíos semejantes, la utilización de servicios de telecomunicaciones que implique una tarificación adicional al afectado o cualesquiera otros medios que impliquen un coste adicional al interesado. 2. El responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde el de la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a lo dispuesto en el artículo 16.3 de la Ley Orgánica 15/1999, de 13

El RGPD consagra que el interesado, afectado o titular de los datos, pueda revocar el consentimiento para el tratamiento de dichos datos en cualquier momento, mientras que nuestra LOPD condicionaba dicha revocación o retirada a la existencia de una causa justificada para la revocación y a que la revocación no tuviera efectos retroactivos. La primera de estas condiciones establecidas en nuestra LOPD, es muy restrictiva. Ha sido superada en el RGPD, pues expresamente se declara en éste la libertad de poder hacerlo «en cualquier momento». Es decir, por un mero acto o una declaración de voluntad, sin tener que alegar o probar la existencia de una causa justificada, al igual que no tuvo que alegar ni probar una causa el interesado para prestar su consentimiento.

En cuanto a la forma de la revocación o retirada del consentimiento, el RGPD dice solo que «será tan fácil retirar el consentimiento como darlo», mientras que la LOPD no dice nada al respecto. Por otro lado, recalcar que, a excepción del RLOPD, ninguna norma de las comentadas recoge nada sobre el coste económico de la revocación o la retirada del consentimiento para el tratamiento de los datos.

1.8 Consentimiento del menor

El RGPD[278] introduce novedades relacionadas con el consentimiento de los menores. La primera gran diferencia es que el RGPD eleva la edad del

---

de diciembre. 3. Cuando el interesado hubiera solicitado del responsable del tratamiento la confirmación del cese en el tratamiento de sus datos, éste deberá responder expresamente a la solicitud. 4. Si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre».

[278] Artículo 8 Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información «1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó. Los Estados miembros podrán establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. 2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales

consentimiento de los menores a los 16 años, frente a los 14 años previstos en la normativa española[279].

No obstante, el RGPD deja margen de libertad a los Estados miembros para establecer por ley una edad inferior a tales fines, siempre que esta no sea inferior a 13 años. Por tanto, si no hay modificación al respecto, en España, la edad seguirá siendo los 14 años.

La segunda diferencia respecto al RLOPD es que el RGPD no se refiere al tratamiento de los datos de los menores en general, sino solo «en relación con la oferta directa a niños de servicios de la sociedad de la información», pero, en la práctica, no tiene mucha trascendencia, al no hacer distinciones de supuestos la normativa española.

La tercera diferencia es que el RGPD es más flexible y más realista en lo que se refiere a la comprobación de la edad del menos y la autenticidad del consentimiento, de los padres o tutores. Así, mientras el RLOPD exigía al responsable del fichero o tratamiento «articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menos y la autenticidad del consentimiento prestado, en su caso, por los padres, tutores

---

casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible. 3. El apartado 1 no afectará a las disposiciones generales del Derecho contractual de los Estados miembros, como las normas relativas a la validez, formación o efectos de los contratos en relación con un niño».

279 En relación al consentimiento para el tratamiento de datos de menores de edad, el artículo 13 RLOPD declara que «1. Podrá procederse al tratamiento de los datos de los mayores de catorce años con su consentimiento, salvo en aquellos casos en los que la Ley exija para su prestación la asistencia de los titulares de la patria potestad o tutela. En el caso de los menores de catorce años se requerirá el consentimiento de los padres o tutores. 2. En ningún caso podrán recabarse del menor datos que permitan obtener información sobre los demás miembros del grupo familiar, o sobre las características del mismo, como los datos relativos a la actividad profesional de los progenitores, información económica, datos sociológicos o cualesquiera otros, sin el consentimiento de los titulares de tales datos. No obstante, podrán recabarse los datos de identidad y dirección del padre, madre o tutor con la única finalidad de recabar la autorización prevista en el apartado anterior. 3. Cuando el tratamiento se refiera a datos de menores de edad, la información dirigida a los mismos deberá expresarse en un lenguaje que sea fácilmente comprensible por aquéllos, con expresa indicación de lo dispuesto en este artículo. 4. Corresponderá al responsable del fichero o tratamiento articular los procedimientos que garanticen que se ha comprobado de modo efectivo la edad del menor y la autenticidad del consentimiento prestado en su caso, por los padres, tutores o representantes legales».

o representantes legales», el RGPD solo le pide que «haga esfuerzos razonables, teniendo en cuenta la tecnología disponible, para verificar, en tales casos, que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño». Estos esfuerzos razonables no deberían limitarse tan solo a la comprobación de la autenticidad del consentimiento de los padres o tutores, sino ampliarse también a la comprobación de la edad del menor.

1.9 Categorías especiales de datos personales

Las excepciones al consentimiento del interesado establecidas en el artículo 6.2 LOPD, no se aplican al tratamiento de datos especialmente protegidos, que encuentran su regulación en el artículo 7[280] LOPD, donde se establece la legitimación para su tratamiento.

---

[280] La LOPD regula los datos especialmente protegidos en su artículo 7, y lo hace en los siguientes términos: «1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando

La protección de los datos de ideología, religión o afiliación sindical representa también en este caso una garantía institucional de la libertad ideológica o religiosa. De igual forma, los datos de raza, salud y vida sexual también merecen una especial protección, ya que esta información forma parte del núcleo más íntimo y reservado de una persona.

La propia Directiva 95/46/CE establece en su artículo 8[281] como regla general la prohibición de tratamiento de estos datos, salvo que se establezcan

---

el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento».

[281] Véase el Artículo 8 Directiva 95/46/CE sobre el tratamiento de categorías especiales de datos «1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. 2. Lo dispuesto en el apartado 1 no se aplicará cuando: a) el interesado haya dado su consentimiento explícito a dicho tratamiento, salvo en los casos en los que la legislación del Estado miembro disponga que la prohibición establecida en el apartado 1 no pueda levantarse con el consentimiento del interesado, o b) el tratamiento sea necesario para respetar las obligaciones y derechos específicos del responsable del tratamiento en materia de Derecho laboral en la medida en que esté autorizado por la legislación y ésta prevea garantías adecuadas, o c) el tratamiento sea necesario para salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento, o d) el tratamiento sea efectuado en el curso de sus actividades legítimas y con las debidas garantías por una fundación, una asociación o cualquier otro organismo sin fin de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refiera exclusivamente a sus miembros o a las personas que mantengan contactos regulares con la fundación, la asociación o el organismo por razón de su finalidad y con tal de que los datos no se comuniquen a terceros sin el consentimiento de los interesados, o e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial. 3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional sea en virtud de la legislación nacional, o de las normas establecidas por las autoridades nacionales competentes, o por otra persona sujeta asimismo a una obligación equivalente de secreto. 4. Siempre que dispongan las garantías adecuadas, los Estados miembros podrán, por motivos de interés público importantes, establecer otras excepciones, además de las previstas en el apartado 2, bien mediante su legislación nacional, bien por decisión de la autoridad de control. 5. El tratamiento de datos relativos a infracciones, condenas penales o medidas de seguridad, sólo podrá efectuarse bajo el control de la autoridad pública o si hay previstas garantías específicas en el Derecho nacional, sin perjuicio de las excepciones que podrá establecer el Estado miembro basándose en disposiciones nacionales que prevean garantías apropiadas y específicas. Sin embargo, sólo podrá llevarse un registro completo de condenas penales bajo el control de los poderes públicos. Los Estados miembros podrán establecer que el tratamiento de datos relativos a sanciones administrativas o procesos civiles se realicen

garantías suficientes. En idéntico sentido, lo reconoce el artículo 6[282] del Convenio 108 del Consejo de Europa de 1981.

La definición de estos datos como especialmente protegidos tiene como consecuencias, sobre todo en lo que hace referencia al consentimiento para el tratamiento. Los datos de ideología, afiliación sindical, religión o creencias solo podrán ser tratados con el consentimiento expreso y por escrito del afectado[283].

El propio artículo 7 establece en su apartado primero que «nadie puede ser obligado a declarar sobre su ideología, religión o creencias», por lo que cuando se proceda a recabar el consentimiento se advertirá al interesado de su derecho a no prestarlo, no pudiendo sustituirse este consentimiento por una ley.

Como regla general, son pocos los tratamientos de datos referentes a la ideología, la religión o las creencias que lleva a cabo la Administración. No obstante, es preciso recordar la salvedad que establece la Directiva 95/46/CE, y es que la letra e) del artículo 8.2 expresamente permite el tratamiento de este tipo de datos, siempre que éste «se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial».

---

asimismo bajo el control de los poderes públicos. 6. Las excepciones a las disposiciones del apartado 1 que establecen los apartados 4 y 5 se notificarán a la Comisión. 7. Los Estados miembros determinarán las condiciones en las que un número nacional de identificación o cualquier otro medio de identificación de carácter general podrá ser objeto de tratamiento».

[282] Por lo que atañe a las categorías particulares de datos, el artículo 6 del Convenio 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal «Los datos de carácter personal que revelen el origen racial, las opiniones políticas, las convicciones religiosas u otras convicciones, así como los datos de carácter personal relativos a la salud o a la vida sexual, no podrán tratarse automáticamente a menos que el derecho interno prevea garantías apropiadas. La misma norma regirá en el caso de datos de carácter personal referentes a condenas penales».

[283] Véase el artículo 7.2 LOPD.

Los datos de carácter personal que hagan referencia al origen racial, a la salud o a la vida sexual «solo podrán ser recabados, tratados y cedidos cuando así lo disponga una ley o el afectado consienta expresamente»[284]. A diferencia de los datos de ideología, religión o creencias, la necesidad del tratamiento de datos de salud para el cumplimiento de determinadas funciones impide supeditarlo al consentimiento del interesado, por lo que basta que exista una previsión legal. La principal diferencia entre una tipología de datos y otra, dentro de su consideración como especialmente protegidos, proviene de la propia previsión constitucional de prohibir la recogida de datos de ideología, religión o creencias sin consentimiento del interesado y previa advertencia de su derecho a no prestarlo.

Por otro lado, el artículo 6.2 LOPD ha establecido de forma expresa que «no será preciso el consentimiento cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6». Éste prevé el tratamiento de los datos especialmente protegidos cuando dicho tratamiento sea necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o los tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento se realice por un profesional sanitario sujeto a secreto profesional o por otra persona sujeta a una obligación idéntica de secreto[285].

---

[284] Véase el artículo 7.3 LOPD.

[285] Una previsión semejante se encuentra en el Reglamento 45/2001/CE, de 18 de diciembre de 2000, del Parlamento Europeo y del Consejo, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. «Artículo 10 Tratamiento de categorías especiales de datos 1. Se prohíbe el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. […] 3. El apartado 1 no se aplicará cuando el tratamiento de datos resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos sea realizado por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación de secreto equivalente». Sin embargo, el contenido de esta norma puede verse modificado ya que previsiblemente, este Reglamento será modificado en un breve periodo de tiempo. Con fecha 10 de enero de 2017, la Comisión Europea presentó una Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la

Igualmente, el artículo 8 LOPD vuelve a afirmar expresamente que las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes «podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad».

Los tratamientos de datos especialmente protegidos tienen que ser respetuosos con el principio de calidad. No solo es necesario respetar las reglas relativas al consentimiento; hay que tener en cuenta que no se deben tratar datos especialmente protegidos si no son claramente adecuados y pertinentes para la finalidad, debiendo ser diligente el responsable del fichero para cancelar la información cuando haya dejado de ser necesaria.

El segundo párrafo del artículo 7.6 LOPD señala que podrá llevarse a cabo un tratamiento de datos especialmente protegidos «cuando sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento». Del mismo modo, la letra f) del artículo 11.2 LOPD legitima la cesión de datos de salud sin consentimiento del interesado

---

Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE, COM(2017) 8 final. Ésta afectará expresamente al apartado que comentamos, pues el artículo 10 de la Propuesta se refiere al tratamiento de categorías especiales de datos personales en los siguientes términos: «1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: […] c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento». De este modo, cambia el punto sobre el que gira la aplicación de la prohibición del tratamiento de este tipo de categoría de datos. Si actualmente se hace depender de que este tratamiento «sea realizado por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación de secreto equivalente», con esta reforma la aplicación de la prohibición del tratamiento de este tipo de datos, descansará en que el sujeto no se encuentre «física o jurídicamente incapacitado para dar su consentimiento». Accesible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52017PC0008&from=EN

«cuando es necesario para solucionar una urgencia que requiera acceder a un fichero»[286].

Con respecto a los datos especialmente protegidos de nuestra LOPD, el RGPD[287] presenta algunas diferencias con trascendencia para el consentimiento.

---

[286] En el mismo sentido, la letra c) del artículo 8.2 de la Directiva 95/46/CE prevé la posibilidad de tratamiento de categorías especiales de datos cuando el mismo sea necesario para «salvaguardar el interés vital del interesado o de otra persona, en el supuesto de que el interesado esté física o jurídicamente incapacitado para dar su consentimiento».

[287] El artículo 9 RGPD versa sobre el tratamiento de categorías especiales de datos personales en los siguientes términos «1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación(es) sexuales de una persona física. 2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes: a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado; b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado; c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento; d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados; e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos; f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial; g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado; h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3; i) el tratamiento es necesario

La primera novedad es que el RGPD incluye dentro de estas categorías especiales de datos personales dos nuevas categorías: i) datos genéticos; y, ii) datos biométricos dirigidos a identificar de manera unívoca a una persona física.

La segunda novedad es que, aunque estas categorías especiales de datos pueden ser tratadas con consentimiento explícito del interesado, se prevé que el Derecho de la Unión o de los Estados miembros puedan impedir que el interesado lo preste.

Por último, la tercera novedad es que, aunque el apartado 2.a) del artículo 9 del RGPD requiere un consentimiento explícito del interesado para tratar estas categorías especiales de datos, sin embargo, el apartado 2.e) permite el tratamiento si el interesado los ha hecho manifiestamente públicos. Lo cual plantea la duda de si el RGPD admite un consentimiento tácito o si ello se considera «una clara acción afirmativa».

---

por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional, j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. 3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes. 4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud».

1.10 Conclusiones

El consentimiento constituye un elemento fundamental para garantizar el poder de disposición y control sobre los propios datos personales.

Uno de los objetivos declarados del RGPD ha sido el reforzamiento de los derechos de los ciudadanos y un mayor control sobre sus datos personales, jugando el consentimiento del titular de los datos un papel fundamental en dicho reforzamiento. En este sentido, la idea era clarificar las normas en materia de consentimiento, para garantizar que se preste de manera informada y libre. El RGPD mantiene las condiciones básicas para considerar válidamente prestado el consentimiento, específico, libre, informado e inequívoco, y sobre las que no se había planteado anteriormente especial discusión.

Sin embargo, se ha comprobado la falta de «libertad» a la hora de prestar el consentimiento en aquellos supuestos en que exista un desequilibrio en las posiciones de las partes. En estos supuestos, el consentimiento no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal. Además, se establece una presunción general por la que se considera que el consentimiento no se ha dado libremente cuando no se permita autorizar por separado las distintas operaciones de tratamiento de datos personales.

En donde sí ha existido tradicionalmente mayor discusión es en el aspecto relativo a la forma de prestar el consentimiento. De la idea inicial de consentimiento explícito, contenida en la propuesta del RGPD, se retorna a un consentimiento inequívoco, tal y como ya recoge actualmente la Directiva 95/46/CE. La desaparición del RGPD del término «explícito», entendido como un «consentimiento expreso», implica un menor grado de protección del titular de los datos. No obstante, el mantenimiento del término «inequívoco» para el consentimiento, al acompañarlo en la definición que lo conceptúa como una «declaración o una clara acción afirmativa», necesariamente debe llevar a que desaparezcan de nuestro ordenamiento prácticas generalizadas de admisión del silencio como base para el

tratamiento de datos personales con consentimiento del titular. Por tanto, ya no será válido en consentimiento válido.

Por otro lado, el RGPD incide en otras cuestiones para reforzar los derechos de los ciudadanos en relación con el consentimiento para el tratamiento de sus datos personales. Así, en la información que debe facilitarse a la hora de prestar el consentimiento, o en el ejercicio de derechos como el de oposición, cancelación o en la revocación del consentimiento. En relación con la primera, se insiste tanto en los aspectos formales, claridad, accesibilidad, y visibilidad de la información, como en el propio contenido de la información, en cuando elementos fundamentales para considerar que nos encontramos ante un auténtico consentimiento informado y, por tanto, válido.

2 EL MITO DEL CONSENTIMIENTO Y EL FRACASO DEL MODELO INDIVIDUALISTA DE PROTECCIÓN DE DATOS

Se ha indicado en el apartado anterior que lo único que legitima un tratamiento de información personal, salvo que una ley disponga de otra cosa, es la voluntad libre e inequívoca de su titular.

Con la reforma del marco europeo de protección de datos, el debate político y regulativo tiene uno de sus focos en ese planteamiento, consentimiento como medio básico de control, y se discute qué noción de consentimiento cuadra mejor con el incesante avance socio-tecnológico.

Pues bien, OLIVER LALANA y MUÑOZ SORO[288], plantean que, la concepción «individualista» que subyace a este enfoque protector no sirve en un mundo de computación ubicua donde las prácticas de obtención y

[288] Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi, p. 154.

análisis masivo de datos son inevitables y banalizas la idea del tratamiento «consentido».

2.1 La ambivalencia del consentimiento

El radio de acción del consentimiento como fundamento del tratamiento de datos personales, se ha visto limitado en los últimos años. Las habilitaciones legales, explícitas o no, para los tratamientos inconsentidos son tantas que, más que la regla, el consentimiento parece casi la excepción[289].

Según la literatura de protección de datos, el principio del consentimiento persigue que la información sobre una persona sea procesada cuándo, cómo y para los fines que ella autorice. Sobra decir que el consentimiento ha de ser informado, de modo que se conozca la finalidad y el alcance del tratamiento. Lo que se pretende es asegurarnos el máximo control posible, y esa parece ser la función clave que debería cumplir.

Es natural que cada cual decida qué se hace con sus datos[290], y que la legislación ampare su margen decisorio. El valor que damos a la privacidad puede oscilar mucho según las circunstancias y los entornos en que actuamos, como también lo hacen nuestras preferencias y deseos sobre el uso que otros pueden hacer de nuestros datos.

---

[289] Las excepciones en el ámbito estatal han crecido de manera sobresaliente en el marco de la cruzada por la seguridad pública, pero también ganan peso las excepciones en el ámbito privado, como ilustran, a título de ejemplo, la STJUE de 24 de noviembre de 2011, en los asuntos Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado, y la STS 429/2012, de 8 de febrero, de la Sala Tercera del Tribunal Supremo, por la que se anula el artículo 10.2b) del Real Decreto 1720/2007, de 21 de diciembre.

[290] El propio Grupo del artículo 29 lo ha defendido en el Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011. WP187. pp 9-10. «Por lo general, el concepto de consentimiento está vinculado a la idea de que el interesado debe controlar el uso que se hace con sus datos […] El consentimiento está relacionado con el concepto de autodeterminación. La autonomía del interesado es a la vez condición previa y una consecuencia del consentimiento: permite al interesado influir sobre el tratamiento de los datos». Accesible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_es.pdf.

De ahí que la ley no imponga de forma taxativa y para cualquier contexto todas las condiciones del tratamiento, sino que admita cierta dosis de flexibilidad y permita modular el régimen legal de acuerdo a la voluntad del titular de los datos. Debemos ser nosotros quienes decidamos sobre nuestra información[291].

Sin embargo, hay una serie de factores que, al sumarse, convierten la norma del consentimiento en algo parecido a una trampa. En lugar de proporcionarnos el control de nuestros datos, asegura su flujo constante y su libre aprovechamiento por empresas y organizaciones.[292]

El margen decisorio del titular de los datos es virtualmente incondicional, sin límites. Mediante el consentimiento se puede legitimar casi cualquier tratamiento. Es verdad que existen muchas normas de obligado cumplimiento para quienes procesan datos personales. Pero solo algunas son definitivamente vinculantes, otras normas son vinculantes de un modo «menos intenso», y pueden sortearse si el interesado consiente. En este sentido, resultan negociables o disponibles. Y como no suelen existir

---

[291] Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi, p. 156.

[292] Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea COM (2010) 609 final, pp. 8-9. «El ejemplo de las redes sociales es especialmente esclarecedor a este respecto, ya que presenta grandes dificultades para que los individuos puedan ejercer un control efectivo sobre los datos que les conciernen. […]Además, en el medio en línea –vista la opacidad de las políticas de confidencialidad– las personas tienen a menudo más dificultades para informarse de sus derechos y dar un consentimiento informado. Esto es tanto más complejo debido a que, en algunos casos, no está claro lo que constituye un consentimiento libre, específico e informado respecto del tratamiento de datos, como en el ámbito de la publicidad en línea basada en el comportamiento, donde se considera a veces, pero no siempre, que los parámetros del navegador del internauta expresan su consentimiento. Conviene pues clarificar las condiciones del consentimiento del interesado, con el fin de garantizar que se concede siempre con conocimiento de causa, y de garantizar que el interesado es plenamente consciente de que da su autorización y respecto a qué tratamiento, de conformidad con lo dispuesto en el artículo 8 de la Carta de los Derechos Fundamentales de la UE».

limitaciones temporales, autorizarlo durante todo el tiempo durante el que sirva a una finalidad legítima del responsable[293].

Por último, sería ingenuo asumir que todos los tratamientos que legalmente se reputan consentidos, ni siquiera los consentidos de manera expresa, se corresponden con nuestras preferencias y son fruto de una «libre elección genuina»[294], y ello sin entrar a valorar cómo afectan ciertos contextos a la prestación del consentimiento. Por un lado, a menudo no somos muy conscientes del verdadero alcance del tratamiento que «autorizamos»: aun cuando el responsable nos informe, podemos ignorar o malinterpretar la

---

[293] Al exigir al responsable que informe del periodo de almacenamiento de los datos, el RGPD parece apuntar en la línea de una limitación temporal. En este sentido, frente a la visión estática del consentimiento como acto aislado y único, resulta más razonable una concepción dinámica basada en la idea de «consentimiento en curso» Whitley, E.A. y Kanellopoulou, N. (2010). Privacy and informed consent in online interactions: Evidence from expert focus groups. *Association for Information Systems. ICIS 2010 Proccedings*, p. 1 y ss. Recuperado de http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1132&context=icis2010_submissions

[294] Así, el propio Grupo de Trabajo del artículo 29, declara en el Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), de 15 de febrero de 2007. WP131. pp 9-10, «un elemento importante es que, para ser válido, el consentimiento - independientemente de las circunstancias en que se exprese - debe ser una "manifestación de voluntad, libre, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernan", según lo definido en la letra h) del artículo 2 de la Directiva. a) El consentimiento debe darse libremente: el consentimiento "libre" supone una decisión voluntaria, de un individuo en posesión de todas sus facultades, tomada sin ningún tipo de coacción, ya sea social, financiera, psicológica u otra. El consentimiento dado bajo amenaza de no tratamiento o de tratamiento de menor calidad en una circunstancia médica no puede considerarse "libre". No se puede considerar váli o el consentimiento dado por un interesado que no haya tenido la oportunidad de hacer una verdadera elección o que se haya encontrado frente a un hecho consumado. […] El recurso al consentimiento debe limitarse a los casos en que el interesado tenga una auténtica libertad de elección y por tanto sea posteriormente capaz de retirar el consentimiento sin sufrir perjuicio alguno. b) El consentimiento debe ser específico: el consentimiento "específico" debe referirse a una situación bien definida y concreta en que esté previsto el tratamiento de datos médicos. Por tanto, un "acuerdo general" del interesado […] no constituiría consentimiento con arreglo a lo dispuesto en la letra h) del artículo 2 de la Directiva. c) El consentimiento debe ser con conocimiento de causa: un consentimiento "informado" por parte del interesado supone un consentimiento basado en la apreciación y comprensión de los hechos y consecuencias de una acción. El individuo afectado debe contar con información exacta y completa, dada de forma clara y comprensible, sobre todas las cuestiones pertinentes, en especial las especificadas en los artículos 10 y 11 de la Directiva, tal como la naturaleza de los datos tratados, los fines del tratamiento de que van a ser objeto los datos, los destinatarios de los mismos y los derechos del interesado. Esto incluye también el conocimiento de las consecuencias de no consentir el tratamiento de los datos en cuestión».

información. Podemos no leer o no comprender las cláusulas de privacidad[295]. Por otro lado, las condiciones de tratamiento raras veces se pactan de modo individual, sino que suelen formar parte de contratos tipo que hemos de aceptar en bloque[296].

Es cierto que podemos ejercer nuestros derechos y facultades de control más tarde, pero no lo es menos que pocas personas se toman la molestia. Siguiendo a OLIVER LALANA y a MUÑOZ SORO, revocar las autorizaciones «formales» para adecuarlas a nuestras preferencias pueda resultar inviable en la práctica –basta imaginar cuánto nos costaría revocar

---

[295] Leith, Ph. (2008). Privacy as Slogan. En Saarenpää, A. (Ed.), *Legal* privacy, Zaragoza: Prensas Universitarias, p. 98. En particular, el conocimiento social de la industria de la información y la minería de datos es escasa, y los datos se recopilan y procesan de maneras que sorprenderían a quienes otorgan si consentimiento.

[296] Los usos y cesiones que no sean necesarios no pueden quedar autorizados por defecto. El artículo 15 RLOPD lo declara de manera expresa: «si el responsable del tratamiento solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos»; Además, en caso de revocarse el consentimiento para una cesión, el responsable debe comunicarlo a todos los cesionarios, quienes deberían cancelar los datos recibidos. Así se manifiesta en el artículo 17.4 RLOPD: «si los datos hubieran sido cedidos previamente, el responsable del tratamiento, una vez revocado el consentimiento, deberá comunicarlo a los cesionarios, en el plazo previsto en el apartado 2, para que éstos, cesen en el tratamiento de los datos en caso de que aún lo mantuvieran, conforme al artículo 16.4 de la Ley Orgánica 15/1999, de 13 de diciembre». Pero la primera de estas normas, aparte de que vincula solo a responsables sujetos a nuestra legislación, deja abierto qué sea o no necesario; por no decir que hay ocasiones en que no estamos realmente en disposición de oponernos al tratamiento, si de ello se siguen consecuencias adversas. La segunda norma queda en nada si la cesión ha sido a países sin adecuado nivel de protección. En relación a la fijación unilateral de las condiciones de uso y privacidad, la AEPD ha señalado expresamente que: «la fijación unilateral de las condiciones de uso y privacidad afecta a la información que reciben los usuarios -deficiente en cuanto a su claridad y accesibilidad- a las finalidades del tratamiento de los datos y a sus plazos de conservación. Con la circunstancia adicional de que dichas políticas se modifican periódicamente siendo también esta modificación una decisión unilateral de quienes ofrecen los servicios […]La fijación unilateral de las condiciones de uso por los prestadores de servicios en Internet hace necesario, junto a las políticas reactivas, primar políticas activas dirigidas a mejorar las garant.as para la protección de los datos personales, especialmente en relación con los menores y las redes sociales». *Memoria de la Agencia Española de Protección de Datos 2010* pp. 26-27.

o precisar los consentimientos que hemos prestado en Internet durante el último mes.

Y eso no es todo, pues por una parte, se ha de sopesar el valor de la ganancia inmediata frente al de una pérdida de control sobre sus datos cuyo efecto es más diferido o difuso –o al revés, sopesar una ganancia difusa de control sobre la información con una pérdida más inmediata–. De otra, juega aquí nuestra tendencia a dar un mayor peso, negativo, a las pérdidas que peso, positivo, damos a las ganancias, según muestra la teoría prospectiva en relación con nuestra aversión a la pérdida o desposesión: valoramos más aquello que ya tenemos, endowment effect. Incluso para una persona que en principio objetaría a ciertos fines o cesiones no imprescindibles para la gestión de su solicitud, un simple acto de revocación puede quedar excluido debido a barreras psicológicas[297].

Siempre le queda la opción de buscar otros oferentes, si no quiere renunciar por razones de privacidad al bien o servicio que desea. Lamentablemente, no será extraño que las prácticas de protección de datos que sigan otras entidades se parezcan mucho a las que la solicitante quería evitar, con lo que, por más que le preocupe la privacidad, es posible que tienda a resignarse.

Así, la regla del consentimiento, cuyo sentido ideal era garantizarnos el control sobre nuestra información, termina amparando una renuncia a la posibilidad real de controlarla; una renuncia a lo que un modelo «fuerte» de protección de datos debería salvaguardar: la autodeterminación informativa[298].

---

[297] Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi, p. 159.

[298] El Grupo del artículo 29 ha manifestado en su Dictamen 15/2011 sobre la definición del consentimiento, de fecha 13 de julio de 2011. WP187 que «si se utiliza correctamente, el consentimiento es un instrumento que permite al interesado controlar el tratamiento de sus datos. Si se utiliza de forma incorrecta, el control por el interesado resulta ilusorio y el consentimiento deja de ser una base adecuada del tratamiento». En idéntico sentido, véase el Dictamen 06/2014 sobre el

2.2 El mantra del control

Nuestro sistema de protección de datos se articula alrededor de un ideal que se ha convertido en un mito: que en la sociedad actual cualquiera pueda mantener un control razonablemente amplio sobre su información personal. Esto es, a grandes rasgos, lo que vienen a prometer las leyes. Pero esta promesa resulta inviable, y a veces parece acercarse peligrosamente al terreno del engaño ideológico. En este sentido, la legislación muestra su cara más simbólica, expresando nobles propósitos que nunca logra transformar en hechos.

Las leyes españolas y europeas proclaman un nivel de garantía de la autodeterminación informativa que a duras penas se refleja luego en la práctica. Esta situación donde el derecho realmente no garantiza lo que promete, o no puede hacerlo, provoca que la «privacidad» y el «control» de la información personal degeneren en un simple eslogan. Como observa LEITH, el discurso legal y oficial persigue «un patrón, control sobre la información personal mediante elecciones personales» que ya es inalcanzable en un mundo basado en el almacenamiento y cruce de datos; y de ahí que «quienes se suban al carro de este eslogan» corran el riesgo de que sus criterios no sirvan para este mundo y se pierda la confianza en ellos[299].

La nueva legislación europea está llamada a encarar el dilema de la pérdida de control del individuo sobre su información personal. Ya desde la evaluación de impacto que acompaña a la propuesta del nuevo RGPD, se denuncian los crecientes impedimentos para que un individuo normal pueda controlar sus datos en un contexto globalizado donde las técnicas de intercambio, generación de perfiles automáticos y minería de datos son cada

---

concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE, de 9 de abril de 2014. WP217.

[299] Leith, Ph. (2008). Privacy as Slogan, en A. Saarenpää, A. (Ed.), *Legal* privacy, Zaragoza: Prensas Universitarias, p. 99.

vez más sofisticadas e invisibles[300]. Y de ahí que un objetivo principal de la reforma sea la recuperación del control individual sobre la propia información, en especial en entornos digitales.

---

[300] Véase al respecto el documento «Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data». SEC (2012) 72 final, 25 de enero de 2012, pp 21-23. «Furthermore, individuals are often neither aware nor in control of what happens to their personal data and therefore fail to exercise their rights effectively. Globalisation and technological developments, particularly the fact that personal data are nowadays being transferred across an increasing number of virtual and geographical borders in the online economy, including through "cloud computing", further challenge the control individuals may keep over their own data. a) Insufficient awareness, loss of control and trust, particularly in the online environment In the online environment, it is increasingly difficult for individuals to be aware of the processing of the data related to them and the risks linked to such processing, to maintain control over their own data and, ultimately, to assert their rights vis-à-vis data controllers. Two thirds of European citizens feel that the disclosure of personal data is a major concern for them and six in ten citizens consider that nowadays there is no alternative to disclosing personal data in order to obtain products and services. Three quarters of citizens feel that they have either no or only partial control of their personal data on social networking sites. – Insufficient awareness and underestimation of privacy risks. In order to be in control, individuals need to be aware by whom, on what grounds, from where, for what purposes, and for how long their personal data are being processed and what their rights are in relation to the processing. Currently, the duty to inform the data subject does not cover each of these elements; and even when sufficient information is available, it is often not understandable for the individual. When they are provided, online privacy policy notices ("Privacy Statements") are often overly complex, making use of technical and legal terminology. This complexity is reflected in the responses to a 2011 Eurobarometer survey: close to six in ten internet users claim they read privacy policies (58%), but only a third say that they read them and understand them (34%); a quarter say that they read them but do not fully understand them (24%). A quarter say they do not read them (25%), one in twenty say they do not know where to find them (5%) and almost one in ten ignore privacy statements (8%). The lack of readily available and easily understandable information makes it difficult for individuals to become aware of the risks linked to the use of their personal data and take the necessary measures to ensure their own protection. For instance, almost half of the respondents to a recent Eurobarometer do not feel sufficiently informed on social networking and file sharing sites. – Loss of control and trust. As confirmed by a recent Eurobarometer survey, profiling, data mining, and technological developments that ease the exchangeability of personal data make it even more important for individuals to be in control of their personal data. The graph below shows the extent to which individuals feel in control of their personal data online. In a recent Eurobarometer survey, 75% of respondents that owned an account on a social networking site and 80% of online shoppers consider that they have no or only partial control over their personal data. 70% of them are concerned that

Declaran OLIVER LALANA y MUÑOZ SOROS[301] que uno de los caminos para lograr ese objetivo se hace pasar por el reajuste de la regla del consentimiento. Para que la decisión individual de aceptar un tratamiento de datos no acarree renunciar al derecho fundamental, se intenta sujetarla a condiciones más rigurosas. Se reproduce el modelo de «consentimiento y control» con el que se busca el «empoderamiento» (empowerment) de los titulares de los datos, es decir, que adquieran o recobren el poder efectivo de decidir qué se hace con su información. A su vez, se quieren redoblar las obligaciones informativas, y quienes procesan datos personales deberán formular las cláusulas de privacidad en términos más sencillos, pero también más completos.

No está claro si –o en qué medida– esta reforma de las normas de consentimiento contribuirá a asegurarnos, de hecho, un mayor control de nuestra información, pero la experiencia reciente quizá no justifica demasiado optimismo. Hasta ahora, la legislación no ha sido capaz de corregir significativamente el rumbo de la voracidad informativa de la sociedad del conocimiento.

Es cierto que el derecho de protección de datos tiene rango fundamental, pero la sociedad parece redefinir sus expectativas de privacidad a la baja, y mucha gente, en sus conductas cotidianas, tiende a poner las ventajas reales o presuntas del flujo libre de datos personales muy por encima de la autodeterminación informativa. Por otro lado, la población cada vez parece más convencida de que la pérdida de privacidad es inevitable, y casi todos tendemos a aceptarla[302]. Asistimos a un paulatino alejamiento entre el ideal

---

economic operators processing their personal data may use it for a different purpose than the one they were collected for».

[301] Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi, p. 164.

[302] Véase Agencia Vasca de Protección de Datos. (2008). Percepciones y actitudes sobre la protección de datos personales. Vitoria: Gobierno Vasco, pp. 27-29. «La protección de datos solo es percibida como una cuestión de gravedad cuando interviene la dimensión económica, relacionada con robos,

de control que se establece en la legislación, y lo que la privacidad supone de veras en la práctica para la mayoría de las personas.

Esa divergencia entre promesa legal y plasmación real nos debería hacer reflexionar. Además, la creciente sofisticación de los tratamientos y la proliferación de decisiones automatizadas cada vez dificultan más que una persona pueda conocer lo que verdaderamente se está haciendo con su información, con sus datos[303].

---

fraudes. Existen niveles de precaución muy acentuados cuando se pone en riesgo la economía de las personas, tarjetas de crédito, cuentas bancarias, etc. El resto de las principales manifestaciones que aparecen en el discurso, publicidad dirigida, telemarketing, etc, son entendidas en clave de molestias, incomodidades, leves perturbaciones, pero no como un problema de primero orden. A medida que va apareciendo el alcance real de las posibles consecuencias asociadas al tema, se produce un tránsito desde la falta de implicación hacia la toma de conciencia de las posibles consecuencias de una indebida gestión en la utilización de datos. Desde la percepción del manejo indebido de datos como una molestia casi inevitable, se evoluciona a una sensación de vulnerabilidad centrada en la gran cantidad de datos que transitan de cada persona en distintas esferas». Recuperado de http://www.euskadi.eus/contenidos/documentacion/cuaderno_sociologico_vasco_25/eu_cu_soc25/adjuntos/csv25.pdf

[303] Con fecha 16 de mayo de 2017, la Autoridad Francesa de Protección de Datos, CNIL, ha hecho pública una sanción a las empresas FACEBOOK INC y FACEBOOK IRELAND. A raíz de la declaración de FACEBOOK relativa a la modificación de su política de privacidad en 2015, la CNIL realizó inspecciones para verificar la conformidad de la red social con la ley francesa de protección de datos. Estas acciones son parte de una iniciativa europea que implica a cinco autoridades de protección también han decidido investigar (Francia, Bélgica, Holanda, España y la Tierra de Hamburgo) sobre las prácticas de Facebook. Los controles llevados a cabo por la CNIL han identificado la existencia de numerosas violaciones de la Ley de Protección de Datos. En particular, Facebook: i) procede a una recopilación de toda la información que tiene sobre los titulares de cuentas para mostrar publicidad orientada sin tener base legal para ello. De hecho, si los usuarios tienen medios para controlar la exhibición de la publicidad dirigida, no se les solicita el consentimiento para la compilación masiva de sus datos y no pueden oponerse a la misma, a la hora de crear su cuenta o en un momento posterior; y ii) procede a un seguimiento injusto de los usuarios de Internet a través de la cookie "datr". El anuncio de ésta, y la mención de la información recopilada "dentro y fuera de Facebook", no permite entender claramente a los usuarios que sus datos son sistemáticamente almacenados cuando naveguen a una página web de terceros. Por lo tanto, la recopilación masiva de datos realizada a través de la cookie "datr", es ilícita debido a la falta de información clara y precisa. En relación a otras infracciones, CNIL considera que las empresas: i) no proporcionan información directa a los usuarios de Internet sobre sus derechos y el uso que se hará de sus datos, en particular en el formulario de inscripción al servicio; ii) recopilan datos confidenciales de los usuarios sin obtener su consentimiento explícito. De hecho, no se facilita a los usuarios información específica sobre el carácter sensible de los datos cuando completan sus perfiles con dichos datos; iii) al utilizar la configuración del navegador web, no permiten que los usuarios se opongan válidamente a las cookies

Conforme el discurso oficial, el problema es que las TIC, las tecnologías de la información y las comunicaciones, avanzan muy rápido y el derecho no logra contenerlas; así, se reclaman nuevas leyes que nos permitan recuperar el control de nuestro destino informacional. En cambio, según el discurso hegemónico de la industria de la información, el problema se encuentra en el propio derecho y en el ánimo iusfundamentalista de los defensores de la privacidad, que marcarían unos límites obsoletos y trasnochados al progreso y la innovación[304], así como a otras libertades, derechos e intereses constitucionales[305]. Y lo que es peor: el derecho de la protección de datos impediría dar a la gente lo que de verdad quiere, libertad, seguridad y eficiencia, y limitaría las elecciones soberanas de los individuos[306].

Los conservacionistas quieren hacer efectivo el control que permite la ley reforzando el modelo de consentimiento informado, mientras que los

---

instaladas o alojadas en sus equipos terminales; y, iv) no demuestra la necesidad de conservar la totalidad de las direcciones IP de los usuarios a lo largo de la vida de su cuenta. En consecuencia, CNIL ha decicido imponer una sanción de 150.000 euros a las empresas FACEBOOK INC y FACEBOOK IRELAND. El texto completo de la misma puede consultarse en https://www.cnil.fr/sites/default/files/atoms/files/san-2017-006.pdf

[304] Tene, O y Polonetsky J. (2012). Privacy in the Age of Big Data. A Time for Big Decisions. *Stanford Law Review online, 63*, pp 68-69: « Privacy advocates and data regulators increasingly decry the era of big data as they observe the growing ubiquity of data collection and the increasingly robust uses of data enabled by powerful processors and unlimited storage. Researchers, businesses, and entrepreneurs vehemently point to concrete or anticipated innovations that may be dependent on the default collection of large data sets. We call for the development of a model where the benefits of data for businesses and researchers are balanced against individual privacy rights. Such a model would help determine whether processing can be justified based on legitimate business interest or only subject to individual consent, and whether consent must be structured as opt-in or opt-out». El texto accesible en https://iapp.org/media/presentations/12Summit/S12_De-identification_HANDOUT_1.pdf

[305] El discurso a favor del progreso se adorna con un discurso paralelo relacionado con el libre flujo del conocimiento y el carácter colectivo, social y dinámico de la información y, por tanto, de la información personal.

[306] Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi, pp. 166-167.

integrados venden también un modelo de privacidad basado en la decisión libre de las personas. Ahora bien, el sistema individualista, centrado en la idea de controlar nuestro destino informacional como individuos, no servirá de mucho cuando ese control no se puede controlar. El ideal normativo de consentimiento y control es un mito. Una persona corriente no puede esperar tener un control sustancial de su información, ni de cómo la usan otros.

2.3 El consentimiento en la cultura de protección de datos

2.3.1 La influencia de las opiniones y los conocimientos

El hecho de que haya muchos ciudadanos para los que el bien jurídicamente protegido tiene escaso valor, sobre todo cuando se confronta con otros posibles beneficios, propicia que las iniciativas empresariales más agresivas en materia de protección de datos encuentren siempre un amplio nicho entre la población que las acepta de forma acrítica, permitiendo de esta forma que se consoliden. Luego, se produce un efecto de adhesión por el que los ciudadanos situados en posiciones intermedias van asumiéndolas paulatinamente.

El consentimiento que se presta en materia de protección de datos tiene un marcado componente ideológico, está relacionado con las opiniones y las actitudes. Es así porque las consecuencias prácticas, y en particular las económicas, aparecen lejanas o muy difuminadas, o simplemente no son percibidas por los ciudadanos.

Aunque en la discusión teórica sobre protección de datos se ponga el énfasis en conflictos de valores como el que se da entre seguridad y privacidad, lo cierto es que en la práctica estos conflictos son resueltos por el legislador, sin que opere el principio de consentimiento, ya que en estos casos los tratamientos son, por lo general, autorizados por una norma. Por tanto, el principio opera normalmente en la elección del ciudadano de consentir el tratamiento de sus datos a cambio de poder acceder a determinados servicios o de obtener algunas ventajas económicas. Ello da lugar a una asimetría, ya que la respuesta afirmativa al consentimiento solicitado sí está vinculada a consecuencias prácticas inmediatas y con contenido económica,

mientras que los motivos para no dar el consentimiento son únicamente de tipo ideológico.

2.3.2 Algunas prácticas relativas al consentimiento

Existen divergencias entre el nivel de preocupación y concienciación en materia de privacidad y las prácticas reales de los ciudadanos. De la mayor importancia que se da a la privacidad y a la protección de datos desde una perspectiva abstracta no se sigue siempre un aumento claro en la frecuencia e intensidad de las conductas de protección.

En el caso de España, que el ciudadano medio declare estar bastante preocupado «por los riesgos para su privacidad y por la seguridad de sus datos personales» no impide que «el número de accesos a las páginas de las políticas de privacidad» sea «muy bajo, prácticamente marginal»; lo que permitiría a su vez inferir que ese ciudadano, «a pesar de creer lo contrario, desconoce el contenido real y las consecuencias de estas políticas»[307], o no está tan preocupado por ellas como afirma.

---

[307] Discurso del Director de la Agencia Española de Protección de Datos Rallo Lombarte, A. (2008). What do Citizens Know and Feel? What art they fear on new tecnologies? Roma: Conferencia de Autoridades de Protección de Datos y Privacidad, pp 3-4 Dada la importancia del texto señalado para el contenido de este trabajo, procedo a exponer sus ideas principales con mayor extensión «Si pudiéramos resumir los resultados de la encuesta en un breve titular diríamos que "los ciudadanos están bastante preocupados por los riesgos para su privacidad y por la seguridad de sus datos personales generados por las nuevas tecnologías de la información". Es muy probable que los ciudadanos no sepan definir con precisión el alcance y naturaleza del derecho fundamental a la protección de datos pero, podemos estar seguros, de que lo intuyen, reconocen e identifican en cuanto éste es amenazado y puesto en riesgo. Los ciudadanos dicen conocer la existencia de las políticas de privacidad en Internet. Sin embargo, nuestra experiencia práctica nos ofrece una conclusión bien contraria. El número de accesos a las páginas de las políticas de privacidad es muy bajo, prácticamente marginal. Las políticas de privacidad ocupan espacios residuales en los websites y resultan ininteligibles. Por tanto, es evidente que el ciudadano, a pesar de creer lo contrario, desconoce el contenido real y las consecuencias de estas políticas de privacidad. En Internet no puede hablarse de un consentimiento basado en información fiable o confiable. Formalmente, los proveedores de Internet cumplen con su deber de informar, pero la mayor parte de las veces la regla del juego en Internet es clara y se basa en: "o lo tomas o lo dejas" ("take it or leave it clauses"). Por otro lado, los usuarios intuyen que la navegación por Internet deja rastro. Unos pocos expertos saben que sus perfiles de navegación son susceptibles de explotación comercial. Pero, a pesar de ello, son mayoritariamente indiferentes a este riesgo. Estamos ante un gravísimo problema de desconocimiento e ignorancia en el uso de estas tecnologías de Internet. Y la "letra pequeña" de las ilegibles clá sulas

Los sociólogos de la privacidad parecen coincidir en que, incluso cuando una mayoría de personas está preocupada por la privacidad y se considera bien informada sobre sus derechos, se detecta una creencia muy extendida de que las amenazas a la privacidad resultan ya inevitables y que el rápido avance de las TIC hace imposible la adecuada protección de la información personal.

---

generales de contratación para la instalación de software contribuye significativamente a este problema. El ciudadano conoce inmediatamente cualquier nueva tecnología, para él ya no son nuevas. El individuo intuye con bastante claridad los riesgos, está preocupado y exige nuestra actuación. Estamos ante un ciudadano-red en una sociedad-red. Cuando las tecnologías de la información alcanzan el mercado, el ciudadano-red está obligado a negociar y defender su privacidad en condiciones de franca desigualdad y desequilibrio. La negociación en el "mercado de la privacy" favorece y coloca en posición dominante a quien presta un servicio "aparentemente libre" en Internet a cambio de la privacy. Frente a ello, ¿qué reglas debemos aplicar?, ¿el modelo europeo?, ¿debe confiarse en la autorregulación de los proveedores de servicios de Internet?, ¿ha llegado la hora del gobierno del código de la privacidad en Internet? En nuestro modelo europeo, el ciudadano, titular de sus datos personales cuenta con un estándar de protección y ejerce unos derechos que le proporcionan un verdadero control sobre sus datos personales. Pero, la protección de los datos personales preocupa a la sociedad global, en el mundo entero. Al vertiginoso ritmo marcado por la Ley de Moore [Ley creada por el cofundador de Intel, Gordon Earl Moore, que previó en 1965 que el número total de transistores integrados en un circuito sería doblado cada dos años], la garantía reactiva de la privacidad frente cada nueva tecnología emergente siempre llegará tarde. Siempre habrá una nueva tecnología, siempre nos quedará la mitad del camino por recorrer y así hasta el infinito. ¡Siempre llegaremos tarde si sólo buscamos reaccionar frente a los riesgos ya consolidados! ¿Acaso quienes diseñan e implantan las nuevas tecnologías desconocen los principios de protección de datos personales? ¿no son conscientes de los estándares de seguridad necesarios? ¿Agreden nuestra privacidad de modo consciente? Seguramente, la cuestión no es qué capacidad tenemos para regular una nueva tecnología sino qué criterios jurídicos deben regir el diseño de tecnologías invasivas de la privacidad. Se trata de obtener un complejo equilibrio. La normatividad internacional no debe frenar el impulso creativo, la innovación y el desarrollo económico que deriva de las nuevas tecnologías. Sin embargo, sí debería fijar principios cuyo respeto constituya un mínimo común denominador de obligada atención en el diseño tecnológico. Resulta esencial alcanzar acuerdos que respeten la cultura de la privacy en cada país y en cada región del mundo pero que garanticen un ejercicio efectivo de los derechos de los ciudadanos». Texto accesible en el link http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/speech_roma_es.pdf.

2.4 La limitada virtualidad del consentimiento en los tratamientos de datos de carácter personal en Internet

2.4.1 Introducción

Las cookies se han convertido en un instrumento clave para la operatividad de la navegación en Internet y para el desarrollo de los servicios de la sociedad de la información.

El Grupo de Trabajo del Artículo 29 de la Directiva 95/46/CE ha realizado una buena descripción técnica de las cookies en su Dictamen 2/2010[308]: las cookies dan lugar a que el navegador del equipo en el que están instaladas no se limite a descargar el contenido solicitado por el usuario y que edita el sitio web, sino que intercambie también información sobre la navegación con ese mismo servidor e incluso conecte el equipo con un sitio web distinto, que recibirá la información que contiene la cookie y la que se deriva de ella. Esta información siempre se refiere a los datos de navegación (aunque con diferente alcance dependiendo del tipo de cookie), a la IP y otros datos de

---

[308] "Normalmente funciona así: el proveedor de redes de publicidad coloca una cookie de rastreo en el terminal del usuario la primera vez que este visita un sitio de internet que exhibe un anuncio de su red. La cookie es un texto breve alfanumérico almacenado (y recuperado posteriormente) en el terminal del usuario por el proveedor de la red. En la publicidad comportamental, la cookie permitirá al proveedor de la red de publicidad reconocer a un antiguo visitante que vuelve a dicho sitio o visita cualquier otro sitio asociado de la red publicitaria. La repetición de visitas permitirá al proveedor de la red publicitaria construir un perfil del visitante que se utilizará para producir publicidad personalizada. Como estas cookies de rastreo los coloca una tercera parte distinta del servidor de la web que exhibe el contenido principal del sitio (es decir, el editor), se suelen conocer como «cookies de terceros». La mayoría de los buscadores [navegadores] de internet ofrecer la posibilidad de bloquear las cookies de terceros. Algunos buscadores [navegadores] facilitan sesiones de búsqueda «privada» que destruyen automáticamente todas las cookies creados cuando se cierra la ventana del buscador [navegador]. Algunas redes de publicidad están sustituyendo o complementando sus cookies de rastreo tradicionales con nuevas tecnologías reforzadas de rastreo como los «flash cookies» (objetos locales compartidos). Las «flash cookies» no pueden borrarse con la configuración tradicional de privacidad de un buscador [navegador]. Se ha señalado que las «flash cookies» se han usado explícitamente como herramienta para restaurar «cookies tradicionales» que habían sido rechazadas o borradas por el usuario. Esta práctica se conoce como respawning (reproducción). Salvo que se indique otra cosa, en el presente Dictamen, el término «cookies» designará todas las tecnologías basadas en el principio de almacenamiento y recuperación de la información en el terminal del usuario". Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010 (WP 171), páginas 6 y 7.

conexión, e incluso en algunos casos a información personal del usuario relativa a los formularios y datos facilitados durante la navegación.

Debe tenerse presente que el dictamen referenciado trata específicamente sobre las cookies de las redes de publicidad, pero esta circunstancia no impide que la descripción resulte perfectamente aplicable a cualquier tipo de cookie.

En definitiva, la operativa de las cookies atiende a un esquema muy sencillo: cada vez que el usuario se descarga un nuevo contenido web (acción que puede consistir en la mera actualización de la página que visualiza, en el "envío" de la informació insertada en un formulario, en la descarga de una nueva página mediante un link insertado en la página que está visualizando, o en la inserción de una nueva dirección web en el navegador), el navegador de su equipo intercambia mensajes con el servidor que domina la cookie, que reacciona en consecuencia, facilitando la navegación, actualizando en algunos casos la información que conserva de la cookie (observando al usuario), o descargando incluso contenidos personalizados en el espacio que tenga reservado en la web desde la que se leyó la cookie.

La tecnología permite que esa conexión e intercambio de información no se limite sólo al sitio web donde se instaló la cookie (web "del editor"), sino que tambié es posible que la cookie se active en otros sitios web (webs "de red") y que cause que el equipo del usuario intercambie información con el sitio web que domina la cookie (web "de origen"), que no tiene por qué coincidir con el sitio web del editor.

Además de la diferenciación de las cookies en base a su duración y a quiénes pueden explotarlas, el GT29 y la Agencia Española de Protección de Datos ("AEPD") clasifican tambié las cookies atendiendo a las finalidades para las que sirven.

En el caso del GT29, distingue entre muy diversos tipos de cookies, en principio las de uso más corriente en la industria (cookies de entrada, de autenticación, de seguridad, de sesión de reproductor multimedia, de complemento para intercambiar contenidos sociales, etc.), para determinar en cada una de ellas si aplican o no las excepciones que establece la norma

a la obligación de obtener el consentimiento para el uso de las cookies. Ello choca, sin embargo, con la afirmación que el propio GT29 hace acerca del carácter polivalente de las cookies[309] en el Dictamen 4/2012, que determina que para que una cookie pueda estar exenta del requisito del consentimiento es necesario que todas las finalidades a que se destina la cookie cumplan las condiciones establecidas en la Directiva.

2.4.2 Régimen jurídico de las Cookies en la Directiva

2.4.2.1 El régimen jurídico previo de la reforma

La evolución que ha tenido esta tecnología, que ha incrementado muchísimo la capacidad de extraer y utilizar información sobre la navegación, ha provocado un cambio normativo a nivel europeo que persigue, fundamentalmente, reforzar el papel del consentimiento de los usuarios. La Directiva 2009/136/CE[310] modificó, entre otras, la Directiva 2002/58/CE, que establece el marco regulador respecto de la privacidad en el sector de las comunicaciones electrónicas.

Efectivamente, la Directiva 2002/58/CE regulaba las cookies en su primera versión de forma muy laxa, limitándose a exigir que se facilitara al usuario información suficiente acerca del uso de cookies por parte del servidor.

Este régimen se basaba, por tanto, en el entendimiento de que el usuario suficientemente informado era libre de decidir si aceptaba la condición establecida por el sitio web y descargaba, en consecuencia, el contenido

---

309 "Una cookie puede utilizarse para diversas finalidades, por lo que únicamente podrá estar exento del requisito del consentimiento si todas y cada una de las finalidades para las que se utilice están individualmente exentas del requisito del consentimiento". Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies, adoptado el 7 de junio de 2012 (WP 194), página 6.

310 Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 por la que se modifican la Directiva 2002/22/CE Relativa al Servicio Universal y los Derechos de los Usuarios en Relación con las Redes y los Servicios de Comunicaciones Electrónicas, la Directiva 2002/58/CE Relativa al Tratamiento de los Datos Personales y a la Protección de la Intimidad en el Sector de las Comunicaciones Electrónicas y el Reglamento (CE) no 2006/2004 Sobre la Cooperación en Materia de Protección de los Consumidores. Diario Oficial n° L 337, de 18 de diciembre de 2009, páginas 11 a 36.

que le interesaba ("entraba" en el sitio web) o, en caso contrario, no aceptaba tal condición y no descargaba el contenido[311][312]. En definitiva, la Directiva 2002/58/CE reconocía a los editores la capacidad para imponer la instalación de cookies como condición para el acceso a la información que

---

311 "(24) Los equipos terminales de los usuarios de redes de comunicaciones electrónicas, así como toda información almacenada en dichos equipos, forman parte de la esfera privada de los usuarios que debe ser protegida de conformidad con el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales. Los denominados «programas espía» (spyware), web bugs, identificadores ocultos y otros dispositivos similares pueden introducirse en el terminal del usuario sin su conocimiento para acceder a información, archivar información oculta o rastrear las actividades del usuario, lo que puede suponer una grave intrusión en la intimidad de dichos usuarios. Sólo debe permitirse la utilización de tales dispositivos con fines legítimos y con el conocimiento de los usuarios afectados. (25) No obstante, los dispositivos de este tipo, por ejemplo los denominados «chivatos» (cookies), pueden constituir un instrumento legítimo y de gran utilidad, por ejemplo, para analizar la efectividad del diseño y de la publicidad de un sitio web y para verificar la identidad de usuarios partícipes en una transacción en línea. En los casos en que estos dispositivos, por ejemplo los denominados «chivatos» (cookies), tengan un propósito legítimo, como el de facilitar el suministro de servicios de la sociedad de la información, debe autorizarse su uso a condición de que se facilite a los usuarios información clara y precisa al respecto, de conformidad con la Directiva 95/46/CE, para garantizar que los usuarios están al corriente de la información que se introduce en el equipo terminal que están utilizando. Los usuarios deben tener la posibilidad de impedir que se almacene en su equipo terminal un «chivato» (cookie) o dispositivo semejante. Esto es particularmente importante cuando otros usuarios distintos al usuario original tienen acceso al equipo terminal y, a través de éste, a cualquier dato sensible de carácter privado almacenado en dicho equipo. La información sobre la utilización de distintos dispositivos que se vayan a instalar en el equipo terminal del usuario en la misma conexión y el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión y abarcar asimismo cualquier posible utilización futura de dichos dispositivos en conexiones posteriores. La presentación de la información y del pedido de consentimiento o posibilidad de negativa debe ser tan asequible para el usuario como sea posible. No obstante, se podrá supeditar el acceso a determinados contenidos de un sitio web a la aceptación fundada de un «chivato» (cookie) o dispositivo similar, en caso de que éste tenga un propósito legítimo". Considerandos 24 y 25 de la Directiva 2002/58/CE.

312 "Los Estados miembros velará por que únicamente se permita el uso de las redes de comunicaciones electrónicas con fines de almacenamiento de información o de obtención de acceso a la información almacenada en el equipo terminal de un abonado o usuario a condición de que se facilite a dicho abonado o usuario información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE y de que el responsable del tratamiento de los datos le ofrezca el derecho de negarse a dicho tratamiento. La presente disposición no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar o facilitar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de proporcionar a una empresa de información un servicio expresamente solicitado por el usuario o el abonado". Artículo 5.3 de la Directiva 2002/58/CE antes de la reforma.

ofrecen en su sitio web, estableciendo como única garantía la transparencia mediante la puesta a disposición de información completa.

Sin embargo, la intensificación del uso derivada de la evolución tecnológica de las cookies ha dado lugar a que este régimen no parezca suficiente, y el Parlamento y el Consejo europeos decidieron reforzar la protección de la intimidad de los usuarios de Internet atribuyendo un papel relevante al consentimiento[313].

2.4.2.2 El consentimiento previo e informado

Fruto de la reforma, el artículo 5.3 de la Directiva 2002/58/CE establece en la actualidad como regla general no sólo la obligación de que se informe al interesado y se le facilite un medio sencillo para oponerse a la instalación de cookies, sino que, previamente a la instalación, se solicite su autorización. Este artículo parece aludir al consentimiento explícito cuando requiere que el interesado "haya dado" su consentimiento y, además, establece como única excepción a esta regla el supuesto de que se haya configurado el navegador para aceptar las cookies[314].

---

[313] "Puede que haya terceros que deseen almacenar información sobre el equipo de un usuario o acceder a información ya almacenada, con distintos fines, que van desde los fines legítimos (como algunos tipos de cookies) hasta aquellos que suponen una intrusión injustificada en la esfera privada (como los programas espía o los virus). Resulta, por tanto, capital que los usuarios reciban una información clara y completa cuando realicen una acción que pueda dar lugar a dicho almacenamiento u obtención de acceso. El modo en que se facilite la información y se ofrezca el derecho de negativa debe ser el más sencillo posible para el usuario. Las excepciones a la obligación de facilitar información y proponer el derecho de negativa deben limitarse a aquellas situaciones en las que el almacenamiento técnico o el acceso sean estrictamente necesarios con el fin legítimo de permitir el uso de un servicio específico solicitado específicamente por el abonado o usuario. Cuando sea técnicamente posible y eficaz, de conformidad con las disposiciones pertinentes de la Directiva 95/46/CE, el consentimiento del usuario para aceptar el tratamiento de los datos puede facilitarse mediante el uso de los parámetros adecuados del navegador o de otra aplicación. La aplicación de estos requisitos debe ganar en eficacia gracias a las competencias reforzadas concedidas a las autoridades nacionales". Directiva 2009/136/CE, Considerando 66.

[314] "Los Estados miembros velarán por que únicamente se permita el almacenamiento de información, o la obtención de acceso a la información ya almacenada, en el equipo terminal de un abonado o usuario, a condición de que dicho abonado o usuario haya dado su consentimiento después de que se le haya facilitado información clara y completa, en particular sobre los fines del tratamiento de los datos, con arreglo a lo dispuesto en la Directiva 95/46/CE. Lo anterior no impedirá el posible

Cabe llamar la atención sobre el hecho de que el Grupo de Trabajo del artículo 29 no presta atención a esta aparente contradicción y concluye en su Dictamen 2/2010, sin matización alguna, que el consentimiento necesario para la aceptación de las cookies tiene que ser explícito y previo[315], es decir, una manifestación expresada antes de que se instale la cookie, de modo que los sistemas que se basan en la deducción de la voluntad contenida de forma implícita en el hecho de que no se rechacen las cookies no resulta válido.

Según afirma el Grupo de Trabajo del artículo 29, el sistema de oposición no cumple el requisito de que la prestación del consentimiento tiene que ser previa, porque normalmente este sistema opera mediante la instalación inmediata de las cookies según se descarga la web visitada, ofreciéndose sólo posteriormente la posibilidad de oponerse a ello[316]. No obstante, cabe entender en sentido contrario que si el sistema respetara el orden temporal que establece este artículo no infringiría dicho principio de prelación temporal.

Por otra parte, respecto del requisito de que el consentimiento sea explícito, el Grupo de Trabajo del artículo 29 considera que la mera oposición sí resultaría válida en el caso de que el usuario tuviera formación y experiencia

---

almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario". Artículo 5.3 de la Directiva 2002/58/CE, después de la reforma.

315 «Los proveedores de redes de publicidad ofrecen cada vez más sistemas de exclusión voluntaria que permiten a los usuarios optar por no recibir publicidad a medida. Mediante este sistema, el usuario debe entrar en el sitio de internet del proveedor de la red de publicidad e indicar que opta por rechazar la posibilidad de que se le rastree con fines de que se le suministren anuncios a medida. […] No obstante, tales sistemas no explicitan en principio el consentimiento del usuario. […] el consentimiento implica la participación activa del usuario previa a la recogida y tratamiento de datos». Dictamen 2/2010 (WP 171), p 17. «Los mecanismos para expresar un consentimiento fundamentado y válido deben requerir la acción explícita del sujeto que indique su disponibilidad a aceptar las cookies […]». Dictamen 2/2010 (WP 171), p 26.

316 «El sistema de exclusión voluntaria se refiere frecuentemente a una falta de reacción del usuario después de que ya haya empezado dicho tratamiento». Dictamen 2/2010 (WP 171), p 17.

suficientes que permitieran afirmar que comprende cómo se obtienen los datos mediante las cookies y es consciente de los efectos de su falta de oposición, pero no en el caso de los usuarios corrientes[317]. Es evidente que esta excepción tan casuística tiene un valor muy escaso, pues, además de la dificultad de valorar cuándo se cumplen estas condiciones, sólo cabrá hacerlo a posteriori, caso por caso y en atención a las circunstancias de cada usuario.

En relación con la configuración del navegador, el Grupo de Trabajo del artículo 29 aclara que no es posible presuponer que se ha otorgado el consentimiento cuando se adquiere y utiliza un navegador que, por defecto, acepta las cookies. La Directiva exige un consentimiento explícito, concreto e informado[318]. Por ello, para aplicar esta excepción sería necesario que el navegador estuviera configurado para rechazar las cookies por defecto, de modo que el usuario tuviera que modificar esa configuración.

Además, el Grupo de Trabajo del artículo 29 afirma que el cambio en la configuración del navegador no puede tener la virtualidad de operar como el otorgamiento del consentimiento previo desde el momento en que el usuario no puede saber qué acepta a futuro, ya que no se puede consentir sobre lo que se desconoce[319]. En definitiva, la interpretación del Grupo de Trabajo del artículo 29 parece redundar en el criterio que veíamos anteriormente de que el usuario sea experto.

---

[317] «Solo en casos concretos, muy específicos, puede inferirse un consentimiento implícito. Ello pudiera ser el caso cuando un usuario experimentado, que está al tanto de la práctica de la publicidad comportamental, sabe que puede optar por rechazarla, pero elige ejercitar un acto consciente de no exclusión (especialmente si lo hace antes de que se envíe ninguna cookie al usuario)». Dictamen 2/2010 (WP 171), p 17.

[318] «[…] es una falacia considerar que, de forma general, la ausencia de reacción del usuario (el que no haya configurado el buscador [navegador] para rechazar cookies) supone una indicación clara y sin equívocos de sus deseos». Dictamen 2/2010 (WP 171), p 17.

[319] «Por último, un consentimiento que equivalga a configurar el buscador para que acepte cookies en bloque implica que los usuarios van a aceptar un tratamiento ulterior de los datos, posiblemente sin conocimiento alguno de los fines o usos de la cookie. Un consentimiento en bloque de todo tratamiento ulterior de los datos sin conocimiento de las circunstancias que rodean el tratamiento no puede considerarse consentimiento válido». Dictamen 2/2010 (WP 171), p 16.

En relación con la extensión material del consentimiento el Grupo de Trabajo del artículo 29 invoca el Considerando 25 de la Directiva 2002/58/CE[320] para afirmar que el consentimiento otorgado para la instalación de la cookie incluye también la autorización para que los servidores que pueden leerla (ya sean el de origen o de red) accedan a la información sobre la navegación que acumula esa cookie. El Grupo de Trabajo del artículo 29 hace esta afirmación refirié dose al contexto de la publicidad "comportamental", pero esta conclusión parece perfectamente aplicable a los restantes escenarios.

Por otra parte, respecto de la duración del consentimiento, debemos recordar también que, al referirse a las cookies de redes publicitarias, el Grupo de Trabajo del artículo 29 señala que el consentimiento no puede ser perpetuo, ya que el usuario podría olvidar que ha consentido su uso. En este sentido, el Grupo de Trabajo del artículo 29 recomienda que las cookies expiren al cabo de un año, transcurrido el cual debería solicitarse de nuevo el consentimiento17.

No obstante, sería razonable que este término de expiración no fuera necesario si el usuario recibiera periódicamente recordatorios sobre la cookie o se le recordara permanentemente que la cookie sigue instalada mediante iconos en las páginas de la red, incluyendo información clara acerca de cómo revocar su consentimiento[321].

---

[320] «El Grupo de Trabajo del artículo 29 es consciente de los problemas prácticos que acarrea el recabar consentimiento, especialmente si este es necesario cada vez que se lee un cookie para enviar publicidad a medida. Para obviar este problema, en línea con el considerando 25 de la Directiva sobre privacidad en las comunicaciones electrónicas («el derecho a impedir la instalación de tales dispositivos se pueden ofrecer en una sola vez durante una misma conexión… en conexiones posteriores»), puede entenderse que la aceptación de un cookie por la persona interesada es válida no solo para el envío del cookie sino también para la ulterior recogida de datos derivados de dicho cookie. En otras palabras, el consentimiento obtenido para instalar el cookie y utilizar la información para enviar publicidad a la medida abarcaría ulteriores «lecturas» del cookie que se producen cada vez que el usuario visita el sitio web asociado al proveedor de la red de publicidad que instaló inicialmente el cookie». Dictamen 2/2010 (WP 171), p 18.

[321] "El consentimiento para el control no debe ser «para siempre» sino solo para un período de tiempo limitado, por ejemplo un año. Pasado ese plazo, los proveedores de la red de publicidad necesitarían obtener un nuevo consentimiento. Esto sería factible si las cookies tuviesen un ciclo de vida limitado

No obstante, sería razonable que este término de expiración no fuera necesario si el usuario recibiera periódicamente recordatorios sobre la cookie o se le recordara permanentemente que la cookie sigue instalada mediante iconos en las páginas de la red, incluyendo información clara acerca de cómo revocar su consentimiento. En este sentido, el Grupo de Trabajo del artículo 29 parece alentar el uso de estos "iconos informativos" en su Dictamen 2/2010[322].

Finalmente, cabe también destacar que la Directiva no aclara quién es el sujeto obligado a solicitar y obtener el consentimiento. Este problema se plantea únicamente en el supuesto de que la web de origen no coincida con la web del editor o existan webs de red, capaces de leer la cookie instalada por un tercero. En estos casos, cabe señalar que tanto la web del editor, como las webs de red, como, por supuesto, la web de origen, desempeñan un papel activo en la instalación de la cookie.

La web de origen porque, al dominar la cookie, decide las reglas a que obedece ésta, la información que almacena la cookie y la que recibe dicha web, así como el propósito a que se destina dicha información, incluyendo la posibilidad de que terceros la compartan.

Las webs de red porque, al autorizar a la web de origen para que instale en ellas los dispositivos lógicos necesarios para reconocer la cookie instalada en el equipo del usuario, permiten a ésta obtener así la información sobre la navegación del usuario en su sitio y descargar en el equipo del usuario la información oportuna. Es decir, participan en la decisión de que se realice dicho procesamiento, lo que permite atribuirles responsabilidad respecto del mismo.

---

después de su instalación en el equipo terminal de la persona interesada (y su fecha de caducidad no debiera prolongarse)". Dictamen 2/2010 (WP 171), pá ina 18.

322 "El Grupo de Trabajo del artículo 29 reconoce la labor realizada por asociaciones como The Future of Privacy para fomentar el uso de iconos a efectos informativos". Dictamen 2/2010 (WP 171), p 18, nota a pie de página 35.

En el caso de la web del editor donde se instala la cookie porque, al igual que las cookies de red, facilita a la web de origen la posibilidad de llevar a cabo dicha instalación, además de que, normalmente, pasará a incorporarse a la red de lectura y aprovechamiento de la cookie.

En definitiva, parece lógico afirmar que en cada una de estas webs recae la responsabilidad de cumplir la obligación de obtener el consentimiento informado y previo a la instalación de la cookie.

En este sentido se pronuncia el Grupo de Trabajo del artículo 29, aunque llama la atención el hecho de que, al analizar la responsabilidad de las que aquí denominamos webs de red, el Grupo de Trabajo del artículo 29 afirma que se trata de una responsabilidad menor, aunque no secundaria. No obstante, esto no le impide concluir que también están obligados a atender las garantías de la Directiva[323].

Conforme a este razonamiento, cabe afirmar que todas las entidades implicadas en la instalación y explotación de la cookie tienen la obligación de respetar las garantías aplicables, de forma diferente en cada caso, según la actividad material que desarrolle cada una de ellas. En todo caso, la obligación de informar, la de facilitar la revocación del consentimiento y la de respetar dicha revocación recae sobre cada una de ellas.

---

[323] «Sin embargo, la responsabilidad del editor abarca la primera fase, es decir, la parte inicial del tratamiento de datos, a saber, la transferencia de la dirección IP que se produce cuando las personas visitan sus sitios de internet. Ello es así porque los editores facilitan dicha transferencia y ayudan a fijar los fines para los que se lleva a cabo, que son enviar publicidad a la medida a los visitantes. En resumen, y por dichas razones, los editores tienen cierta responsabilidad en estas acciones como responsables del tratamiento de datos. Responsabilidad, sin embargo, que exige respetar el grueso de las obligaciones contenidas en las Directivas. En este sentido, es preciso interpretar el marco jurídico de modo flexible aplicando solo aquellas disposiciones que sean pertinentes. Los editores no retienen información personal, de modo que no tendría sentido aplicarles disposiciones de la Directiva como el derecho de acceso. Sin embargo, como se concreta a continuación, la obligación de informar a las personas del tratamiento de datos se aplica plenamente a los editores». Dictamen 2/2010 (WP 171), p 13.

2.4.2.3 El derecho de revocación

Ni la Directiva ni el Grupo de Trabajo del artículo 29 realizan mayores precisiones acerca de este derecho, aunque parece evidente que tiene que facilitarse y respetarse la posibilidad de ejercerlo, así como que debe informarse al usuario acerca de cómo hacerlo efectivo.

Ahora bien, en qué forma puede ejercitarse el derecho de revocación en relación con las cookies. No es fácil responder a estas preguntas y entendemos que deben ser las posibilidades técnicas que existan en cada momento las que determinen la forma en que se pueda hacer efectivo este derecho de revocación.

2.4.2.4 Las excepciones al consentimiento

El artículo 5.3 de la Directiva 2002/58/CE establece dos excepciones[324] a la obligación de obtener el consentimiento.

La redacción literal de este artículo solo exceptúa la obligación de obtener el consentimiento, de modo que cabe plantearse la duda de si está o no también exceptuada la obligación de informar en los casos que se regulan. La duda la resuelve el Considerando 66 de la Directiva 2009/136/CE, que afirma que la excepción debe operar respecto de ambas obligaciones. A la vista de dicho considerando, el Grupo de Trabajo del artículo 29 interpreta la excepción en sentido amplio. Si una cookie está exceptuada, no es necesario informar al usuario de su existencia e instalación.

---

[324] Conforme a este apartado, «lo anterior no impedirá el posible almacenamiento o acceso de índole técnica al solo fin de efectuar la transmisión de una comunicación a través de una red de comunicaciones electrónicas, o en la medida de lo estrictamente necesario a fin de que el proveedor de un servicio de la sociedad de la información preste un servicio expresamente solicitado por el abonado o el usuario».

2.4.2.4.1 Cookies necesarias para la transmisión de una red de comunicaciones electrónicas

Esta primera excepción, afirma el Grupo de Trabajo del artículo 29, opera en relación con "cualquier tipo de intercambio de datos que se produzca mediante el uso de una red de comunicación electró ica".

El Grupo de Trabajo del artículo 29 precisa en su Dictamen 4/2012[325], que, para poder calificarla de necesaria, la transmisión de la comunicación electró ica "no debe ser posible sin el uso de la cookie". Es decir, si fuera posible llevar a cabo la transmisión sin instalar una cookie, la excepción no operaría y sería necesario obtener el consentimiento para su instalación.

Sobre este último punto, y a título de ejemplo, el Grupo de Trabajo del artículo 29 aclara que los elementos que pueden entenderse "absolutamente necesarios" para una transmisión a través de una red entre dos partes pueden ser: i) "la capacidad de enviar la información a través de la red, especialmente mediante la identificación de los extremos de la comunicación"; ii) "la capacidad de intercambiar datos en su orden previsto, especialmente mediante la numeració de paquetes de datos"; y iii) "la capacidad de detectar errores de transmisión o pérdidas de datos".

El Grupo de Trabajo del artículo 29 propone, por tanto, una interpretación muy estricta de esta excepción.

2.4.2.4.2 Cookies necesarias para la prestación de un servicio expresamente solicitado por el usuario

Respecto de la segunda excepción, el Grupo de Trabajo del artículo 29 propone también una interpretación restrictiva, remarcando como requisitos necesarios para su aplicació que el usuario realice una "acción positiva para solicitar un servicio con un perímetro claramente definido" y que, al igual

---

[325] Dictamen 4/2012 sobre la exención del consentimiento de cookies, de 7 de junio de 2012. WP 194. Recuperado de http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_es.pdf

que respecto de la primera excepción, no sea posible prestar el servicio sin la cookie.

Ahora bien, como un servicio de la sociedad de la información suele estar constituido por diversos componentes, el Grupo de Trabajo del artículo 29 aclara que la excepción no puede aplicarse a los servicios considerados en su conjunto, sino a cada una de las «funcionalidades específicas» efectivamente solicitadas por el interesado de forma activa.

Esta interpretación restrictiva afecta, no solo al sitio web que domina la cookie, sino también a los demás corresponsables de ésta, como son el sitio web del editor y los sitios web de la red que también explotan la cookie. En consecuencia, cualquier entidad que se adhiera a una red de cookies debe informarse cuidadosamente acerca de las características técnicas de las cookies que se instalan o utilizan en su web a fin de comprobar que no participa en una utilización abusiva de la cookie.

2.4.2.5 La interpretación de la AEPD

En España, el Real Decreto-ley 13/2012[326] implementó en el artículo 22.2 LSSI[327] los cambios establecidos en la Directiva 2009/136/CE, mediante la transcripción casi literal del texto establecido en esa Directiva. Esta modificación entró en vigor el 1 de abril de 2012.

Pues bien, a pesar de que la modificación de norma española es un reflejo fiel de lo dispuesto en la norma europea, transcurrió más de un año desde su entrada en vigor para que la AEPD publicase su Guía sobre el uso de las cookies, que vio la luz el 29 de abril de 2013. No obstante, a partir de la publicación de la Guía sobre el uso de las cookies, hemos observado como

---

[326] Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista. Boletín Oficial del Estado nº 78, de 31 de marzo de 2012, páginas 26.876 a 26.967.

[327] Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico. Boletín Oficial del Estado nº 166, de 12 de julio de 2002, páginas 25.388 a 25.403.

muchas páginas web, en su gran mayoría pertenecientes a grandes empresas, han incluido secciones en sus condiciones generales de uso en las que se informa de forma detallada sobre el uso de cookies y que "asaltan" al usuario mediante ventanas emergentes que le advierten sobre el uso de cookies. Sin embargo, el grado de incertidumbre jurídica, aunque menor, sigue existiendo.

El 14 de enero de 2014, casi dos años después de la entrada en vigor del actual artículo 22.2 de la LSSI, la AEPD ha dictado una resolución sancionadora aplicando por primera vez este artículo.

La resolución reitera, de forma más resumida, la clasificación por tipos o categorías de las cookies que ya recogió la guía de la AEPD, que había simplificado la clasificación realizada por el GT29 en el Dictamen 4/2012. Esta clasificación distingue entre diversos tipos de cookies a la vista de algunas de sus características o de la finalidad para que sirven (cookies propias o de terceros; cookies de sesión o persistentes; y cookies técnicas, de personalización, de análisis, publicitarias y de publicidad "comportamental").

En este sentido, las cookies llamadas de publicidad "comportamental" estarán exceptuadas si se instalan para atender la solicitud del usuario de recibir un servicio que consiste precisamente en recibir publicidad personalizada. La cookie sería necesaria para atender dicha solicitud y, por tanto, aplicando los principios interpretativos analizados a lo largo de este documento, no sería siquiera obligatorio advertir de su uso, bastando con la solicitud del servicio concreto por parte del usuario.

Por tanto, el alcance de la excepción de la necesidad de la cookie para la prestación del servicio solicitado por el usuario puede ser amplísimo, máxime a la vista del concepto de servicios de la sociedad de la información que establece la LSSI[328]. De este modo, la obligación de informar y recabar

[328] El apartado a) del Anexo LSSI define como «Servicios de la sociedad de la información» o «servicios»: todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario. El concepto de servicio de la sociedad de la información

el consentimiento explícito queda prácticamente sin contenido, ya que el editor de la web podrá optar entre ofrecer abiertamente el servicio que pretenda prestar y que precise necesariamente de la cookie, o prestarlo sin que lo solicite el interesado, pero informando sobre la cookie y recabando el consentimiento para instalarla.

La AEPD desarrolla con mucho más detalle la forma en que debe atenderse el deber de informar que establece el artículo 22.2 de la LSSI, dando mayor certeza a los requisitos que ya recogía la Guía sobre el uso de las cookies.

La información, señala la AEPD, debería darse en dos capas: una primera capa con información muy extractada que el usuario vería al acceder al sitio web (una ventana emergente, por ejemplo), y una segunda capa permanentemente accesible mediante un link con información completa.

La primera capa de información, señala la AEPD, tiene que incluir como mínimo una advertencia sobre el uso de cookies no exceptuadas del consentimiento, la identificación de sus finalidades, la indicación de si es propias o de terceros, la advertencia de qué acción concreta del usuario se interpreta como la prestación del consentimiento y un link a la segunda capa[329].

La AEPD aplica, por tanto, la excepción del artículo 5.3 de la Directiva (22.2 párrafo 3 de la LSSI) tanto al deber de informar como al de solicitar el consentimiento previamente a la instalación de las cookies.

---

comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios».

[329] La primera capa debería incluir la siguiente información mínima: i) Advertencia sobre el uso de cookies no exceptuadas que se instalan al navegar por los sitios web o al utilizar el servicio solicitado; ii) Identificación de las finalidades de las cookies que se instalan, con información sobre si se trata de cookies propias o de terceros; iii) Advertencia, en su caso, de que si se realiza una determinada acción se entenderá que el usuario acepta el uso de las cookies; iv) Un enlace a la segunda capa informativa en la que se indica una información más detallada. Esta información es necesaria para que el usuario conozca el uso de estos dispositivos, su finalidad, los responsables de su utilización y la conducta de la que se inferirá la prestación del consentimiento, así como para que éste pueda obtener información adicional". Resolución R/02990/2013, en el PS/00321/2013, pá ina 27.

Respecto de las finalidades, la AEPD no exige que en esta primera capa se facilite información exhaustiva, sino una descripción muy concisa. Así, la resolución califica como suficiente la indicación de que las cookies de una página web analizada sirven "para recopilar informació estadística sobre su navegación para poder mostrarle publicidad relacionada con sus preferencias".

En cuanto a la acción concreta que pueda interpretarse como aceptación de las cookies, la AEPD reitera la necesidad de que el consentimiento sea explícito. Sin embargo, no exige que el usuario pulse un botón de "Aceptar", sino que parece admitir implícitamente, aunque no expresamente como hacía en su guía, que la mera acción de continuar navegando sirve como manifestación de la aceptación a la instalación de cookies.

Además, la AEPD no menciona en la resolución la exigencia que incluyó en la Guía sobre el uso de las cookies, relativa a que en los casos en que la manifestación de consentimiento no sea "expresa", debe insertarse un aviso permanentemente visible que advierta acerca de las cookies en la página web. Es más, ni siquiera parece que la AEPD exija su aplicación[330].

En la segunda capa, es necesario incluir, según indica la AEPD, la definición y función de las cookies, el tipo de cookies, su finalidad, la forma de desactivarlas o eliminarlas y la forma de revocar el consentimiento, y la identificación de quiénes las utilizan, incluidos los terceros con los que se haya contratado la prestación de un servicio que suponga el uso de cookies.

La definición de las cookies indicando su función, conforme a la Guía sobre el uso de las cookies, se cumpliría mediante una breve introducción a las

---

[330] Efectivamente, en su Resolución, la AEPD no aprecia que haya motivos para sancionar cuando: «Estos avisos, que contienen la información mínima exigible en la primera capa, se mantienen visibles hasta que el usuario acepta la «Política de Cookies» o realiza la acción requerida a los efectos de la obtención del consentimiento», sin hacer ninguna referencia a que existan o no iconos o banners permanentes. op. cit.

cookies. Esto es, parece que la AEPD requiere que se explique qué son y para qué sirven de forma teórica.

Al exigir que se indique el tipo de cookies, la AEPD pide que se atienda a la clasificación que ella misma realiza, según se desprende de la resolución y de la guía.

En relación con el deber de informar sobre la finalidad de las cookies entendemos que solo alcanza a las cookies no exceptuadas, conforme al Considerando 66 de la Directiva 2009/136/CE, aunque la AEPD no lo precisa y, sin embargo, sí lo hace al describir los requisitos de la primera capa.

De la resolución y de la guía de la AEPD se desprende que la información debe ser completa, clara y suficientemente explicativa, aunque no necesariamente extensa. Es más, entendemos que el exceso de información puede determinar el incumplimiento de este requisito. Ahora bien, la AEPD no despeja las dudas relativas a qué nivel de detalle considera suficiente.

En relación con el derecho de revocación y la forma de desactivar o eliminar las cookies, la AEPD hace referencias que parecen indicar que se trata de dos supuestos diferentes. Sin embargo, tanto la guía, como la resolución tratan estos supuestos de forma unificada, dando a entender que estos derechos se atienden mediante la indicación genérica de que el usuario puede bloquear o eliminar las cookies de su equipo y, además, incluyendo links con información específica sobre la forma de eliminación en distintos navegadores. Podemos entender, por tanto, que se trata de un solo supuesto.

Por último, el deber de identificar quiénes utilizan las cookies incluye, según la AEPD, la identificación de las entidades que gestionan las denominadas cookies de terceros. Sin embargo, la AEPD no se plantea que la información sobre quiénes utilizan las cookies puede englobar, en el supuesto de las cookies compartidas, a múltiples entidades (caso de redes de publicidad y otros supuestos análogos). Lógicamente, la exigencia de que se informe sobre la totalidad de los miembros de la red puede resultar imposible, ya que el editor de la página web posiblemente no tendrá esa información.

No obstante, el Grupo de Trabajo del artículo 29 pone de manifiesto en su Dictamen 2/2010[331] que basta con hacer una «referencia explícita a la red de publicidad que está instalando» y la AEPD parece seguir este mismo criterio en la resolución[332], puesto que solo menciona como constitutivo de la infracción la falta de identificación de la entidad que domina la cookie.

Dado que el deber de información tiene que adecuarse a la LOPD, según establece el artículo 22.2 de la LSSI, resulta necesario, tanto indicar la denominación social del tercero como su dirección.

A la hora de valorar la claridad de la información facilitada al usuario, la AEPD considera necesario que la información se concentre en dos capas y que no esté dispersa en diversos documentos.

2.4.3 Conclusión

La reforma de la Directiva 2002/58/CE ha establecido un régimen de consentimiento explícito, previo e informado para la instalación y uso ulterior de las cookies. Las únicas excepciones a esta regla operan en aquellos casos en que las cookies son estrictamente necesarias para transmitir una

---

[331] «Los buscadores [navegadores], juntos o en combinación con otras herramientas de información, incluida la cooperación de proveedores de redes de publicidad y editores, deben transmitir información clara, completa y perfectamente visible para garantizar que el consentimiento está plenamente fundamentado. Para cumplir lo dispuesto en la Directiva 95/46/CE, los buscadores [navegadores] deben transmitir, en nombre del proveedor de la red de publicidad, la información pertinente sobre el objeto de las cookies y el tratamiento de datos ulterior. Las advertencias genéricas sin referencia explícita a la red de publicidad que está instalando la cookie no son, pues, suficientes». Dictamen 2/2010 (WP 171), página 16.

[332] «Por lo tanto, no contiene una información adecuada sobre el tipo de cookies que efectivamente se utilizan y sus finalidades que permita conocer al usuario de una forma apropiada el uso que se dará a la información recuperada, tampoco se asocia claramente su uso con el propio editor o con terceros que también deben ser identificados, habiéndose constatado que sólo se hace referencia a las cookies del servicio Google Analytics de Google Inc sin citar otras cookies de terceros cuya descarga también se ha comprobado se realiza en los terminales de los usuarios, como son, por ejemplo, las de Automattic Inc, Quantcast, YouTube LLc, Zopim Technologies Pte Ltd, Seevolutión Inc.». Resolución citada, página 31.

comunicación por una red electrónica o atender un servicio expresamente solicitado por el usuario. Ambas excepciones deben interpretarse de forma muy restrictiva conforme afirma el Grupo de Trabajo del artículo 29, en el sentido de que solo operan en el caso de que no sea posible atender dichas finalidades sin usar la cookie correspondiente.

En todo caso, la excepción de la necesidad de la cookie para la prestación del servicio solicitado por el usuario deja prácticamente sin contenido la obligación de informar y recabar el consentimiento.

El Grupo de Trabajo del artículo 29 y la AEPD han determinado también la necesidad de permitir al usuario revocar su consentimiento inicial por medio del llamado derecho de revocación, si bien debemos criticar que no se haya establecido con claridad cómo debe hacerse efectivo este derecho en la práctica.

Por último, la AEPD ha descrito con detalle la forma en que debe facilitarse la información para solicitar el consentimiento.

Por lo tanto, a pesar de los evidentes esfuerzos realizados del Grupo de Trabajo del artículo 29 y de la AEPD para aclarar el régimen jurídico aplicable las cookies y establecer unas pautas que faciliten a la industria el cumplimiento de la norma sin perjudicar por lo demás los avances y ventajas que ofrece esta tecnología, existen aún importantes vacíos y dudas en la interpretación de la norma, así como contradicciones que redundan en una grave falta de seguridad jurídica.

En definitiva, deberá ser la evolución de la industria, junto con las resoluciones e informes emitidos por las autoridades de protección de datos, los factores que finalmente perfilen la forma en la que debe aplicarse la norma. Pero lo que nunca debemos olvidar es que a la tecnología no puede ponérsele freno, máxime cuando se convierte en un claro impulsor de la economía.

2.5 Consentimiento «libre» en una relación «desequilibrada»: el interés legítimo

A diferencia de la Directiva 95/46/CE que puso el consentimiento en condiciones de igualdad con otras causas de legitimación, la LOPD partió del consentimiento como regla general y configuró las restantes causas de legitimación como una excepción a este consentimiento.

El papel del consentimiento ha ido ganando peso al tiempo que también ha aumentado la duda sobre su validez por su eventual falta de libertad[333]. Parece que la Comisión ha querido ampliar esta reflexión a otras relaciones donde se entendería que se produce un desequilibrio entre el afectado y el responsable del tratamiento[334]. Sin embargo, esta reflexión simplista es muy

---

[333] Las primeras reflexiones al respecto se situaron en el entorno laboral donde la libertad del consentimiento era cuestionable muchas veces en las relaciones laborales, donde el miedo a la pérdida del puesto de trabajo anularía una manifestación de voluntad libre en materia de protección de datos: «The Article 29 Working Party takes the view that where consent is required from a worker, and there is a real or potential relevant prejudice that arises from not consenting, the consent is not valid in terms of satisfying either Article 7 or Article 8 as it is not freely given. If it is not possible for the worker to refuse it is not consent. Consent must at all times be freely given. Thus a worker must be able to withdraw consent without prejudice. An area of difficulty is where the giving of consent is a condition of employment. The worker is in theory able to refuse consent but the consequence may be the loss of a job opportunity. In such circumstances consent is not freely given and is therefore not valid. The situation is even clearer cut where, as is often the case, all employers impose the same or a similar condition of employment. In other cases the worker should also clearly be provided with information (Article 10) and the Article 7 and Article 8 criteria should be sufficiently broad to legitimise the processing on grounds other than consent». Opinion 8/2001 on the processing of personal data in the employment context, de 13 de septiembre de 2001. WP48. Así, el Grupo de Trabajo del artículo 29 considera que si un empresario debe tratar datos personales como consecuencia inevitable y necesaria de la relación laboral, actuará de forma engañosa si intenta legitimar este tratamiento a través del consentimiento. El recurso al consentimiento deberá limitarse a los casos en los que el trabajador pueda expresarse de forma totalmente libre y tenga la posibilidad de rectificar posteriormente sin verse perjudicado por ello.

[334] Al hablar sobre las condiciones para el consentimiento, el artículo 7 RGPD determina expresamente: «1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. 2.Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento. 3.El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del

peligrosa porque puede llevar a la desaparición del consentimiento como causa de legitimación efectiva.

Muchas de nuestras cláusulas son «desequilibradas» y no por ello se considera que se produce un vicio en el consentimiento que anula el objeto de nuestro «falso» consentimiento. Además, muchas de esas relaciones deben ser desequilibradas para que un negocio pueda funcionar legítimamente. No somos ajenos a la necesidad, y más en el mundo digital, de funcionar con condiciones generales de la contratación.

Es más, por influencia anglosajona, se han impuesto como práctica de mercado contar con unas políticas de privacidad que funcionan como condiciones generales de la contratación y que –en general– pueden combinar dos características: i) contar con los innumerables contenidos que exigen las normas de protección de datos y sus autoridades; y ii) ser a la vez perfectamente incomprensibles.

---

consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo. 4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato». En idéntico sentido, el Considerando 42 establece expresamente «Cuando el tratamiento se lleva a cabo con el consentimiento del interesado, el responsable del tratamiento debe ser capaz de demostrar que aquel ha dado su consentimiento a la operación de tratamiento. En particular en el contexto de una declaración por escrito efectuada sobre otro asunto, debe haber garantías de que el interesado es consciente del hecho de que da su consentimiento y de la medida en que lo hace. De acuerdo con la Directiva 93/13/CEE del Consejo (1), debe proporcionarse un modelo de declaración de consentimiento elaborado previamente por el responsable del tratamiento con una formulación inteligible y de fácil acceso que emplee un lenguaje claro y sencillo, y que no contenga cláusulas abusivas. Para que el consentimiento sea informado, el interesado debe conocer como mínimo la identidad del responsable del tratamiento y los fines del tratamiento a los cuales están destinados los datos personales. El consentimiento no debe considerarse libremente prestado cuando el interesado no goza de verdadera o libre elección o no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno».

Desgraciadamente, las políticas de protección de datos cada vez se alejan más de las sencillas propuestas en 2004 por el Grupo de Trabajo del Artículo 29[335].

La cuestión no es que el consentimiento no deba utilizarse en toda relación «desequilibrada, sino en determinar, en cada contexto desequilibrado, cuándo podemos considerar legítimas las finalidades del tratamiento de los datos de que se trate: es decir, si se trata de i) un uso que no violenta las expectativas razonables del afectado de conformidad con el contexto[336]; o ii) una finalidad «abusiva» que deba prohibirse y no se pueda sanar con un consentimiento.

En sede de protección de datos personales, este análisis solo es posible si se aplica la causa del interés legítimo de la letra f) del artículo 7 de la Directiva 95/46/CE[337]. Fue la Sentencia del Tribunal de Justicia de la Unión Europea, de 24 de noviembre de 2011[338], la que indicó a las autoridades

---

335 Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, WP100, de 25 de noviembre de 2004. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2004/wp100_es.pdf

336 En materia de derechos de propiedad intelectual, es interesante observar la doctrina del «fair use» del derecho de los EE.UU. como una limitación a la regla general de obtener el consentimiento del autor para la explotación de su obra.

337 Artículo 7 «Los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva».

338 Sentencia del Tribunal de Justicia de 24 de noviembre de 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado. «El artículo 7, letra f), de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, debe interpretarse en el sentido de que se opone a una normativa nacional que, para permitir el tratamiento de datos personales necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, exige, en el caso de que no exista consentimiento del interesado, no sólo que se respeten los derechos y libertades fundamentales de éste, sino además que dichos datos figuren en fuentes accesibles al público, excluyendo así de forma categórica y generalizada todo tratamiento de datos que no figuren en tales fuentes». El texto completo de la Sentencia puede consultarse en

administrativas y judiciales españolas que en la LOPD que estaban implementando de forma incorrecta el efecto directo de este artículo. Y es que, aquella incorporó incorrectamente el contenido de dicho apartado de la Directiva 95/46/CE, pues limitó la aplicación de esta causa al hecho de que los datos provinieran de determinadas fuentes denominadas «accesibles al público», que la LOPD reserva a una lista exhaustiva de fuentes públicas. El RLOPD profundizó en este error en la letra b) de su artículo 10.2[339], subsumiendo el «interés legítimo» en las demás causas de legitimación, en lugar de reconocerlo como una causa de legitimación con sustantividad propia.

Sin embargo, el RGPD reconoce en la letra f) del artículo 6.1 que el tratamiento será lícito si «es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño».

---

http://curia.europa.eu/juris/document/document.jsf?text=&docid=115205&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=975959

[339] Artículo 10. Supuestos que legitiman el tratamiento o cesión de los datos. «1. Los datos de carácter personal únicamente podrán ser objeto de tratamiento o cesión si el interesado hubiera prestado previamente su consentimiento para ello. 2. No obstante, será posible el tratamiento o la cesión de los datos de carácter personal sin necesidad del consentimiento del interesado cuando: […] b) Los datos objeto de tratamiento o de cesión figuren en fuentes accesibles al público y el responsable del fichero, o el tercero a quien se comuniquen los datos, tenga un interés legítimo para su tratamiento o conocimiento, siempre que no se vulneren los derechos y libertades fundamentales del interesado. No obstante, las Administraciones públicas sólo podrán comunicar al amparo de este apartado los datos recogidos de fuentes accesibles al público a responsables de ficheros de titularidad privada cuando se encuentren autorizadas para ello por una norma con rango de ley». Este apartado fue anulado por la Sentencia del Tribunal Supremo de 8 de febrero de 2012, de la Sala Tercera.

2.6 Desinformar informando y el «user empowerment»

Es un hecho cierto que, los usuarios, sin leerse ni una sola política de privacidad, que sin embargo aceptan despreocupadamente, proporcionan sus datos personales a cambio de servicios «gratuitos».

Se percibe una asimetría entre la percepción del legislador, de los profesionales, la de las empresas u otras organizaciones que explotan los datos y la de los propios usuarios respecto de las oportunidades y los riesgos del entorno digital y el papel que juegan al respecto la intimidad y la protección de los datos personales.

Desde el legislador se proclama como una máxima que el desarrollo digital requiere crear confianza y que esa confianza solo se consigue con normas más rigurosas de protección de datos que «apoderen» al usuario. Esto es, que den un papel central a su consentimiento expreso, libre específico, informado, y revocable. Un poder del que los usuarios no parecen querer hacer uso confiando en que la legislación evitará los abusos.

Mucho se ha escrito de la necesidad de «apoderar» al usuario en la era digital. Ese «user empowerment» se acaba traduciendo por el legislador en un consentimiento informado, provocando dos consideraciones en relación con la responsabilidad del usuario y en relación con el alcance del deber de informar.

En cuanto a la primera consideración, afirma ÁLVAREZ RIGAUDIAS que el usuario no se toma la molestia de leer las políticas de privacidad. Cuando se las lee es cuando se produce un incidente. Si es consumidor, sabe que puede solicitar ante los tribunales la anulación de las cláusulas generales de contratación que sean abusivas. Sin embargo, la incorrecta información del artículo 5 LOPD no se solventa en los tribunales, ni tiene como consecuencia la nulidad del tratamiento, sino que deriva en una infracción que investiga y sanciona la Autoridad de Control de protección de datos. Lo anterior provoca dos efectos perniciosos:

Las políticas de privacidad no se suelen redactar para el usuario sino para la Autoridad de Control y, por ello, el esfuerzo no se centra en facilitar una

información sencilla, sino en cumplir todos los requisitos de información que la aquella haya podido exigir. A los requisitos de información de protección de datos se yuxtaponen los requisitos de información de las normas de comercio electrónico y servicios de la sociedad de la información y de la normativa de consumidores y usuarios. Estas tres normativas están protegiendo el mismo bien jurídico, pero con requisitos no necesariamente coincidentes ni plenamente compatibles. El resultado no es más que una amalgama de cuantiosa información técnica, esto es, la desinformación.

ii) La organización que capta los datos del usuario no se ve estimulada en diferenciarse frente a sus competidores como «un campeón de la protección de los datos». El usuario no lee nada de las condiciones de los contratos que va a celebrar que no sea el precio. Tampoco percibe que su privacidad puede estar en ocasiones en riesgo, por lo que no discrimina a una empresa frente a otra porque le ofrezca herramientas sencillas y efectivas de gestionar sus preferencias de privacidad.

En términos de protección de riesgos en materia de privacidad, según el contexto, puede ser más efectivo imponer requisitos de Privacy by design o Privacy by default a los creadores de la tecnología, y a quienes la explotan comercialmente, que imponer a los responsables del tratamiento escribir políticas de privacidad, cada vez más largas para dar cumplimiento a mayores deberes de información, que deban ser aceptadas mediante casillas no pre-marcadas.[340]

2.7 Profiling automatizado

Parecemos tener una fe ciega en la tecnología y en los modelos matemáticos. Por ello, acabamos teniendo una fe ciega igualmente en las predicciones que realiza la tecnología. En realidad, la tecnología realiza los

[340] Álvarez Rigaudias, C. (2015). El poder del usuario digital. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo Derecho europeo de protección de datos* Valencia: Tirant lo Blanch, pp 301-302.

cálculos y combinaciones de información de conformidad con unos criterios que unos seres humanos han elaborado. Pero esos criterios no se revisan hasta que se comprueba que la predicción, basada en muchas ocasiones en meras correlaciones, puede ser errónea y causar daños de distinto calado a los individuos.

Muchos de esos daños pueden tener en el balance de los intereses en liza, un impacto «de minimis» y deben ser tolerados en aras del progreso tecnológico y económico. Solo debemos estar alerta cuando lo que se daña es nuestra libertad.

Una de las preocupaciones principales que subyace es la percepción del impacto creciente de la automatización de perfiles en la toma de decisiones relevantes sobre los individuos por parte de las empresas, tal y como lo expresó la Comisión, en relación con los trabajos preparatorios de la Directivo 95/46/CE, en su Comunicación de 24 de septiembre de 1990[341]:

> *«Artículo 14. Derechos complementarios del interesado. […] El apartado 2 del artículo 14 establece que el interesado no puede ser objeto de decisiones de instituciones del sector público o privado que impliquen una apreciación de su comportamiento basada únicamente en un tratamiento automatizado de datos personales que dé un perfil de los datos o de la personalidad del interesado. Con esta disposición se pretende proteger el interés del interesado en aquellas decisiones que sean importantes para él. El uso de perfiles detallados basados en datos personales por parte de importantes instituciones públicas y privadas priva al interesado de la posibilidad de influir en los procesos decisorios de dichas instituciones cuando esas decisiones se toman únicamente sobre la base de su perfil personal».*

[341] Comunicación de la Comisión sobre la protección de las personas en lo referente al tratamiento de datos personales en la Comunidad y a la seguridad de los sistemas de información; Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales. COM (90) 314 final SYN 287 y 288.

Siguiendo las generaciones propuestas por BING[342], uno de los rasgos característicos o definitorios del contexto tecnológico actual es el caracterizado porque los ordenadores son capaces de manejar conocimiento, lo que se logra a través de la tecnología denominada inteligencia artificial. Dentro de ésta, una de las herramientas más utilizadas son las redes neuronales. Se emplean tanto para el correo electrónico, para el profiling, o para el data mining[343], con objetivos como obtener patrones de comportamiento de la población o de grupos.

En la era del Internet de las cosas, en todo momento generamos información relacionada con aspectos de nuestra vida que, combinada y segmentada de acuerdo con determinadas correlaciones, más o menos afortunadas en su capacidad «predictiva», pueden predeterminar sin más que una persona, por la categoría a la que pertenece por «la estadística», pueda acceder o no, a un determinado tipo de producto o servicio.

Todo ello lleva a que el concepto de decisión automatizada vaya incorporándose a nuestro Ordenamiento. El RGPD añade el consentimiento como tercer supuesto legitimador de las decisiones automatizadas[344].

---

[342] Bing, J. (1990). Three Generations of Computerized Systems for Public Administration and Some Implications for Legal Decision-Making, *Ratio* Juris Volume 3 Issue 2, pp. 219-236. Según Bing, hay tres generaciones de los sistemas de información en las organizaciones, la primera orientada a los datos, la segunda a los documentos, y la tercera al conocimiento.

[343] El término se traduce por minería de datos, y en su origen consistía en el aprovechamiento, utilizando técnicas estadísticas y de inteligencia artificial, de los datos utilizados por las organizaciones en la gestión con la finalidad adicional de obtener información útil para el auxilio a la adopción de decisiones.

[344] Así, el artículo 22 RGPD referente a las decisiones individuales automatizadas, incluida la elaboración de perfiles, reconoce expresamente que: «1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar. 2. El apartado 1 no se aplicará si la decisión: a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento; b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o c) se basa en el consentimiento explícito del interesado. 3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a

Anteriormente, la Directiva 95/46/CE indicaba que debían existir medidas que permitan al afectado defender sus intereses, pero no decía nada de que fuera preciso el consentimiento[345]. En este sentido, resultan también inadecuadas medidas de protección como la prevista a nivel interno[346], ya que es difícil pensar que los ciudadanos puedan dedicar el tiempo necesario, ni que dispongan de la formación precisa para poder comprender y valorar la información que se les facilite en el ejercicio de este derecho. No debemos adoptar una completa automatización de procesos en la toma de decisiones

---

impugnar la decisión. 4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado».

[345] Expresamente se declara en el artículo 15 Directiva 95/46/CE, relativo a las decisiones individuales automatizadas, que «1. Los Estados miembros reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc. 2. Los Estados miembros permitirán, sin perjuicio de lo dispuesto en los demás artículos de la presente Directiva, que una persona pueda verse sometida a una de las decisiones contempladas en el apartado 1 cuando dicha decisión : a) se haya adoptado en el marco de la celebración o ejecución de un contrato, siempre que la petición de celebración o ejecución del contrato presentada por el interesado se haya satisfecho o que existan medidas apropiadas, como la posibilidad de defender su punto de vista, para la salvaguardia de su interés legítimo; o b) esté autorizada por una ley que establezca medidas que garanticen el interés legítimo del interesado».

[346] Por lo que se refiere a la impugnación de valoraciones, el artículo 13.3 LOPD recalca que «el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto». Este artículo ha sido desarrollado por el artículo 36 RLOPD referente al derecho de oposición a las decisiones basadas únicamente en un tratamiento automatizado de datos, en los siguientes términos «1. Los interesados tienen derecho a no verse sometidos a una decisión con efectos jurídicos sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, tales como su rendimiento laboral, crédito, fiabilidad o conducta. 2. No obstante, los afectados podrán verse sometidos a una de las decisiones contempladas en el apartado 1 cuando dicha decisión: a) Se haya adoptado en el marco de la celebración o ejecución de un contrato a petición del interesado, siempre que se le otorgue la posibilidad de alegar lo que estimara pertinente, a fin de defender su derecho o interés. En todo caso, el responsable del fichero deberá informar previamente al afectado, de forma clara y precisa, de que se adoptarán decisiones con las características señaladas en el apartado 1 y cancelará los datos en caso de que no llegue a celebrarse finalmente el contrato. b) Esté autorizada por una norma con rango de Ley que establezca medidas que garanticen el interés legítimo del interesado».

que conlleve una consustancial reducción de las responsabilidades del ser humano.

Así, la información sobre la lógica aplicada por estos sistemas puede llegar a ser de una gran complejidad técnica o incluso, como ocurre en el caso de las redes neuronales, de imposible especificación hasta para sus desarrolladores. En consecuencia, la opción de utilizar el consentimiento como medio de control ante la aplicación de las tecnologías más avanzadas para el tratamiento de los datos de carácter personal, choca con una barrera prácticamente insalvable, como es la imposibilidad de que, en supuestos tan complejos, y concibiéndolo como un acto ejercitado individualmente, pueda llegar a lograrse un consentimiento efectivamente informado.

Debemos reflexionar no solo sobre los criterios de segmentación del profiling sino sobre la finalidad de su utilización y el papel que queremos, o no, darle al consentimiento individual. El peor impacto de las decisiones supuestamente racionales de las máquinas que podemos temer es la anulación de nuestra libertad.

3 COMPUTACIÓN UBICUA, PRIVACIDAD Y PROTECCIÓN DE DATOS: OPCIONES Y LIMITACIONES PARA RECONCILIAR CONTRADICCIONES SIN PRECEDENTES[347]

3.1 Introducción

El contexto tecnológico en el que nos encontramos conlleva serias limitaciones al modelo de «consentimiento-control». Aunque podrían señalarse otros rasgos definitorios de este contexto, merece la pena destacar uno de ellos. Me refiero a la computación ubicua[348].

Afirma ČAS, al que por la especificidad del tema a desarrollar, y su interés, seguiremos en la exposición de este apartado relacionado con la computación ubicua, que las tecnologías de computación ubicua poseen el potencial de proporcionar unos niveles anteriormente inconcebibles de apoyo a actividades humanas en distintos aspectos de la vida mediante sistemas que funcionan de forma discreta, basándose en tecnología invisible incorporada en entornos y artefactos del día a día. Los dispositivos de entrada artificiales se sustituyen por interfaces con un lenguaje natural que

---

[347] Čas, J. (2010) «Computación ubicua, privacidad y protección de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes». Revista Española de Protección de Datos. núm. 6, 2010. pp. 69-104.

[348] El concepto de ubicuidad en las TIC fue introducido por Mark Weiser, Weiser, M. (1991). The Computer for the 21st Century. *Scientific American.* pp. 94-104. «Es el acceso a gran cantidad de información y procesamiento de la misma, independientemente de la ubicación de los usuarios. Esto implica la existencia de una gran cantidad de elementos de computación disponibles en un determinado entorno físico y constituido en redes. Los elementos están empotrados o embebidos en enseres, mobiliario y electrodomésticos comunes y comunicados en red inalámbrica por radio frecuencia. La computación ubicua es un modelo de interacción en el que el procesamiento de información se integra fuertemente en las actividades y objetos cotidianos. En lugar de interactuar intencionadamente con un solo dispositivo como sucede hasta ahora, se interactúa con muchos dispositivos simultáneamente, incluso para las tareas cotidianas y en muchas ocasiones sin que la persona sea consciente de ello». Una versión libre del texto completo del artículo puede encontrarse en el link https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf

observan a los usuarios e interpretan palabras pronunciadas, gestos o movimientos como órdenes potenciales.

Mientras que en el pasado, la divulgación de datos se encontraba vinculada principalmente a actividades de las que los interesados eran conscientes y que, por lo tanto, se encontraban, en principio, bajo el control de las personas, el nuevo paradigma les priva de la libertad de tomar dichas decisiones. Por consiguiente, la computación ubicua supone una amenaza sin precedentes no solo para la privacidad, sino para los numerosos componentes de las sociedades.

La principal razón para los límites a la hora de diseñar y concebir sistemas de computación ubicua que respeten la privacidad es el hecho de que esta visión de la tecnología se opone a algunos de los principios más importantes en los que se basa la protección de la privacidad actual.

3.2 Retos a los que nos enfrentamos en materia de privacidad

El enorme incremento de la brecha entre la cantidad y la calidad de los datos que necesitan y generan los sistemas de computación ubicuos y la eliminación simultánea de medios disponibles para controlar la recopilación, el almacenamiento, la transferencia y la utilización de estos datos constituye el reto principal inherente a esta visión.

La difusiónn de tecnologías de la información en red, en las pertenencias personales supone un medio técnico suficiente para establecer una infraestructura de vigilancia que abarque esferas de la vida que hasta el momento permanecían intactas. La vinculación y la fusión de datos procedentes de distintas fuentes y el enriquecimiento mediante sensores que escuchan, miran y observan a seres humanos sin filtro de interfaces técnicas, añade nuevas dimensiones cualitativas a los datos recabados. La capacidad cada vez mayor de almacenar y analizar cantidades enormes de datos no solo amplia la vigilancia del historial de los interesados, sino que también proporciona medios e incentivos para generar predicciones sobre sus futuros comportamientos y necesidades.

3.2.1 Vigilancia ubicua

El incremento en el número de sensores a los que estarán expuestos los interesados que vivan en un entorno de computación ubicua, independientemente de si están incorporados de forma invisible en entornos o en dispositivos personales o pertenencias que se llevan encima, es un factor responsable del incremento correspondiente de los datos generados.

Actualmente, la generación de rastros digitales se restringe, con muy pocas excepciones, a la utilización activa de tecnologías de la información o de las comunicaciones. Una exención importante está relacionada con la información de localización generada por los teléfonos móviles encendidos, ya que se requiere conocer su localización aproximada para encaminar llamadas a las estaciones-base más cercanas. Con la computación ubicua, se invierte la situación habitual; los sensores invisibles observan a los usuarios y los alrededores de forma permanente para prestar servicios o ajustar el entorno de acuerdo con órdenes expresas o necesidades percibidas, interpretando el contexto actual y estableciendo relaciones con las preferencias de sus usuarios, obtenidas a partir de experiencias pasadas y condensadas en perfiles perfeccionados constantemente.

El alcance cada vez mayor que afecta a ámbitos de la vida anteriormente intactos viene acompañado de la imposibilidad de facto de excluirse de ser observado. Renunciar a utilizar dichos servicios con el fin de proteger la intimidad es, por lo tanto, en numerosas situaciones, un concepto teórico más que una alternativa viable, refutándose el requisito de consentimiento informado «libre». El hecho de que pueda protegerse este derecho y en qué grado dependerá de la arquitectura concreta y del diseño del sistema.

3.2.2 Aumento de la calidad de los datos

El aumento de la calidad de los datos describe el incremento en las dimensiones de la información y de las conclusiones que pueden obtenerse en lugar de la exhaustividad, la precisión y la actualización en relación con el fin de la recopilación. Mientras que el incremento en la cantidad

presumiblemente aumente también la exhaustividad, la precisión también puede deteriorarse considerablemente.

El enriquecimiento de contenidos de información es una consecuencia directa de la sustitución de interfaces artificiales como teclados, pantallas táctiles o ratones por interfaces de lenguaje natural u observación mediante vídeo e interpretación de movimientos, gestos o mímica. El cambio de información basada en textos a datos multimedia tendrá como resultado un aumento de la calidad.

La elaboración de perfiles y la extracción de datos crean la amenaza adicional de que incluso datos que, si se tomaran por separado, no tendrían consecuencias desde el punto de vista de la privacidad, podrían volverse muy sensibles. Conjuntos de datos correlativos que podrían considerarse insignificantes o incluso triviales podrían proporcionar información íntima, por ejemplo, acerca del estilo de vida o los riesgos para la salud si se aplica un procedimiento de extracción de datos.

3.2.3 Almacenamiento de datos persistente

El progreso técnico de las tecnologías de almacenamiento permite proporcionar capacidades cada vez mayores a unos costes que disminuyen rápidamente; como consecuencia, las barreras de costes para el almacenamiento a largo plazo de cantidades de datos recabados que crecen exponencialmente también están perdiendo rápidamente su relevancia económica. Se está produciendo un desarrollo similar para capacidades de análisis y tratamiento de datos que permiten aplicar procedimientos de extracción de datos sofisticados a colecciones de datos enormes que anteriormente resultaban inaccesibles a costes razonables en un plazo de tratamiento aceptable.

3.2.4 Repersonalización de datos

En entornos de computación ubicua desaparecerán en gran medida las posibilidades existentes de utilizar los servicios de forma anónima o mediante seudónimos o sencillamente la posibilidad de encontrarse físicamente presente de forma inadvertida en dichos sistemas. Con la

computación ubicua y los numerosos ordenadores o dispositivos incorporados de forma invisible, es el propio usuario el que inicia la recogida y el tratamiento de datos o la prestación de servicios. Por lo tanto, resulta inevitable alguna forma de identificación de la persona que solicita conscientemente o inicia inconscientemente un proceso.

Asimismo, la posibilidad de utilizar identidades falsas se encuentra limitada a causa del proceso de captura de los datos y del tipo de datos necesariamente implicados en este proceso. En general, la computación ubicua solo tiene sentido si los sistemas pueden aprender del pasado, enriquecer y corregir perfiles personales de forma permanente y adaptar los servicios de forma acorde, lo que, a su vez, requiere que se permita que los sistemas «recuerden», es decir, almacenen datos personales. El estado normal de la computación ubicua es que siempre existirán formas de reestablecer la identidad personal de las personas una vez capturada.

La multitud de datos de enlace procedentes de distintas fuentes, sensores y tiempos implica que los datos recabados por sistemas de información ubicua son, en principio, datos personales. La ubicuidad de la recogida de datos también difuminará la distinción entre datos sensibles y no sensibles. En primer lugar, la captura de datos persistente y ubicua también incluirá necesariamente elementos de naturaleza sensible; en segundo lugar, la vinculación y la obtención de conjuntos de datos, consistentes en informaciones personales no vitales, pueden revelar información muy sensible acerca del interesado en cuestión.

3.2.5 Incremento de la asimetría de la información

El deseo de proporcionar inteligencia ambiental de forma discreta requiere un marco en el que los usuarios sean objeto de observación permanente y su comportamiento y acciones se interpreten de forma autónoma, teniendo en cuenta su localización y otra información contextual. A continuación, los resultados se introducen en un proceso de aprendizaje continuo que formará la base para decisiones autónomas del sistema sobre cómo y cuándo utilizar o transmitir la información recabada.

La computación ubicua implica más datos acerca del interesado y, al mismo tiempo, menos transparencia para los usuarios y menos control por parte de éstos; amplía necesariamente la asimetría ya existente en la información y el poder entre los interesados y aquéllos que recaban los datos. Sociedad panóptica

La única actitud realista de los seres humanos que viven en entornos de computación ubicua sería suponer que cualquier actividad o inactividad es objeto de seguimiento, análisis, transferencia y almacenamiento y podría utilizarse en cualquier contexto en el futuro. Nadie puede estar seguro, en ningún lugar, de que sus acciones no están siendo observadas y de que sus conversaciones no están siendo registradas o de que la presencia en cualquier localización no está siendo almacenada en algún registro, ya sean sistemas de computación ubicua sofisticados o mediante simples dispositivos individuales.

3.3 Contradicciones con los fundamentos actuales de la privacidad

Las Directrices[349] sobre la protección de la privacidad y flujos transfronterizos de datos personales fueron desarrolladas por los países miembros de la OCDE y adoptadas con fecha de 23 de septiembre de 1980. Estas Directrices son de aplicación a los datos personales, tanto del sector público como del privado, que, a causa de la manera en que hayan sido tratados, o por su índole o por el contexto en el cual se utilicen, presenten un peligro para la intimidad y las libertades individuales. Las directrices establecen que los siguientes principios deben cumplirse en la recogida y tratamiento de la información personal y los datos[350]:

---

[349] Las directrices aplican para todos los datos personales. Si bien no son jurídicamente vinculantes, han sido reconocidas como una declaración de las normas que deben regir la privacidad de los datos personales y guiar a los miembros de la OCDE y las organizaciones privadas en la elaboración de sus políticas.

[350] El contenido completo de las «Directrices de protección de datos y circulación transfronteriza de datos personales», se encuentran disponibles en el siguiente link

1) Principio de limitación de la recogida: debería haber límites en la recogida de datos personales, y tales datos, deberían recabarse mediante medios lícitos y justos y, en su caso, con el conocimiento o consentimiento del sujeto de los datos.

Principio de calidad de los datos: los datos personales deberían ser pertinentes a los efectos para los que se vayan a utilizar y, en la medida necesaria a tales efectos, deberían ser exactos y completos, y mantenerse al día.

Principio de especificación de la finalidad: los efectos para los cuales se recojan los datos personales deberían especificarse en el momento de la recogida, a más tardar, y la posterior utilización quedar limitada al cumplimiento de tales efectos o de aquellos otros que no sean incompatibles con los mismos y que se especifiquen en cada ocasión en que se cambie la finalidad.

Principio de limitación de uso: los datos personales no deberían revelarse, hacerse disponibles o utilizarse de otro modo a efectos que no sean los especificados conforme al Apartado 9, salvo: a) con el consentimiento del sujeto de los datos, o b) por imperativo legal.

Principio de salvaguardas de seguridad: los datos personales deberían protegerse, mediante salvaguardas de seguridad razonables, frente a tales riesgos como pérdida de los mismos o acceso, destrucción, uso, modificación o revelación no autorizados.

Principio de apertura: debería haber una política general de apertura respecto a avances, prácticas y políticas con respecto a los datos personales. Deberían existir medios fácilmente disponibles para establecer la existencia e índole de los datos personales, y de las principales finalidades para su uso, así como la identidad y domicilio del controlador de los datos.

Principio de participación individual: La persona debería tener derecho a: a) recabar, del controlador de los datos o de otro modo, confirmación de si el

---

http://www.oas.org/es/sla/ddi/docs/Directrices_OCDE_privacidad.pdf. De igual modo, aquellas aparecen publicadas en el año 2013 «The OECD Privacy Guidelines» pp. 14-15. El texto completo se encuentra accesible en http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

controlador tiene o no tiene datos correspondientes a la misma; b) hacer que se le comuniquen los datos correspondientes a ella dentro de un plazo razonable, por una cuota en su caso, que no sea excesiva, de manera razonable y de una forma que le resulte fácilmente inteligible; c) que se le den los motivos para ello, en virtud de los subapartados a) y b), si su solicitud fuere denegada y ella pueda impugnar tal denegación, y d) impugnar los datos que se refieran a ella y, si la impugnación prospera, hacer que se supriman, rectifiquen, completen o modifiquen los mismos.
Principio de responsabilidad: el controlador de datos debería ser responsable del cumplimiento de las medidas que den efecto a los principios expuestos más arriba.

Los conflictos o contradicciones entre la visión de la computación ubicua y los Principios de la OCDE pueden identificarse para los ocho principios indicados en estos principios básicos[351].

3.3.1 Principio de limitación de recogida

La primera parte de este principio hace referencia a una limitación general de la recogida de datos personales. Sin embargo, los datos sobre personas y objetos situados dentro del alcance de los sistemas de computación ubicua se recaban de forma activa, ubicua y continua. Incluso aunque solo se almacene o trate ulteriormente una parte de esta enorme cantidad de

---

[351] Tal y como venimos manifestando a lo largo de todo este trabajo, y siguiendo lo establecido por el RGPD, los principios fundamentales de protección de datos que violan los sistemas de información ubicuos están relacionados con el principio de calidad, e incluyen el principio de minimización de los datos y el principio de finalidad determinada. [Expresamente reconoce el artículo 5 RGPD en relación a los principio relativos al tratamiento que «1.Los datos personales serán: […] b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»)»]. El primero de estos principios constituye una clara contradicción con los incontables procesadores y sensores incorporados de forma invisible que forman los sistemas de computación ubicua. Su limitación haría prácticamente imposible el funcionamiento previsto y la prestación de servicios por parte de sistemas de computación ubicua.

información, se invierte totalmente el principio de limitación de la recogida de datos. La última parte del principio hace referencia al conocimiento y el consentimiento informado de la persona cuyos datos se están recabando. Aunque todavía se puede lograr un conocimiento básico, por ejemplo, mediante etiquetas de advertencia claramente visibles que indiquen que se está utilizando computación ubicua, conocer detalladamente qué objetos capturan, qué tipo de datos, y en qué momento, resulta difícilmente concebible, tanto por motivos prácticos como por su incompatibilidad con el objetivo inherente de discreción.

El requisito de basar el tratamiento de datos personales en el consentimiento inequívoco de los interesados, recogido en el artículo 7 de la Directiva 95/46/CE se vuelve completamente inviable. Asimismo, hoy en día, la condición previa de que el interesado otorgue su consentimiento de forma inequívoca no es posible, ni deseable en todos los casos y en todo momento.

El derecho a la intimidad ya se encuentra hoy permanentemente amenazado por las políticas de seguridad y las tecnologías que se centran en una percepción de seguridad parcial que descuida el papel central de la privacidad para la seguridad de las personas. Sin embargo, estas amenazas aumentarán drásticamente con la computación ubicua, ya que esta tecnología reforzará en gran medida las posibilidades cuantitativas y cualitativas de seguimiento y las ampliará a aspectos que actualmente quedan fuera del alcance de una vigilancia permanente y discreta.

El objetivo de la discreción es completamente incompatible con la adquisición del consentimiento de la persona para cada actividad de recogida de datos; una secuencia de observaciones permanentes conllevaría, del mismo modo, solicitudes de consentimiento permanentes. El desequilibrio en la relación entre la posibilidad de obtener el consentimiento de los interesados, por una parte, y las capacidades de observación de los sistemas de computación ubicua, por otra, promete incrementarse en mayor medida de forma drástica.

Otra preocupación mucho más grave está relacionada con el hecho de que no existe posibilidad de que aquellas partes de la población que no quieran

ser objeto de una observación permanente escapen a la infraestructura de vigilancia. En un entorno de computación ubicua ideal no existe forma de escapar a la vigilancia ubicua. Por lo tanto, la omnipresencia de la computación ubicua presenta la difícil cuestión jurídica de si un «consentimiento libre de dudas» a algo que es inevitable puede considerarse o no como una parte válida de un acuerdo individual o colectivo.

La cuestión del consentimiento en la computación ubicua se complica ulteriormente con la exhaustividad de los datos capturados en lo que se refiere a incluir categorías de datos no sensibles y especiales según se define en la Directiva 95/46/CE. Esta exhaustividad implica que, por una parte, se están capturando directamente datos sensibles. Por otra parte, la vinculación y el análisis de datos que, tomados por separado, no generarían preocupaciones en relación con la privacidad, pueden exponer impresiones muy variadas del interesado, incluyendo datos personales muy sensibles.

3.3.2 Principio de calidad de los datos

Este principio posee dos dimensiones; en primer lugar, la relevancia de los datos para el fin previsto; en segundo lugar, el carácter exacto, completo y actual de los datos. En general, puede esperarse que la computación ubicua tenga como resultado un mejor cumplimiento de las demandas en la segunda dimensión. Sin embargo, solo el conocimiento exacto del sistema concreto que se está utilizando y datos empíricos de instalaciones piloto permitirán realizar afirmaciones válidas sobre estos aspectos de calidad de los datos.

En general, más datos no significa necesariamente mejores datos. Con el fin de obtener datos más precisos, deben existir también controles y correcciones regulares. Este requisito implica otra compensación: sin un almacenamiento central o coordinado de una u otra forma, resultan difícilmente concebibles unos procedimientos de mejora de la calidad, mientras que las recogidas de datos centralizadas suponen una vez más unos enormes incentivos para un elevado riesgo de abuso.

3.3.3 Principio de especificación del propósito

En la base de este principio se encuentra la exigencia de que, como mínimo en el momento de la adquisición de los datos, los fines deben ser conocidos e identificables. Los cambios posteriores en los fines solo se permiten si son compatibles con la intención original; asimismo, deben indicarse adecuadamente.

Sin embargo, el objetivo de las tecnologías de la información ubicuas no es servir a fines únicos y definibles previamente, sino apoyar a los usuarios en diversas situaciones más o menos previsibles. El objetivo de la recogida de datos se basa en su totalidad en la acumulación de tantos datos como puedan tratarse para generar la mayor cantidad de información posible acerca de preferencias y patrones de comportamiento de personas; los contenidos de y el contexto en el que va a aplicarse este conocimiento siguen estando necesariamente poco claros en el momento de la recogida de datos.

La ausencia de un fin específico también elimina un criterio esencial para la evaluación de la legalidad de la recogida de datos por parte de dichos sistemas. Suavizar el requisito de especificidad de una forma suficiente para incluir los sistemas de computación ubicua reduciría la aplicabilidad y la efectividad de esta obligación a un grado casi seguramente inaceptable. La falta de fines específicos elimina la base para determinar si los datos personales son «adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente». Sin un fin, o con un fin especificado de forma demasiado general, también el principio de minimización de los datos y el principio de proporcionalidad, incluidos de forma implícita en el citado requisito, pierden los criterios de evaluación básicos y, por lo tanto, su aplicabilidad.

3.3.4 Principio de limitación de uso

Este principio afirma que los datos no pueden divulgarse, transferirse o utilizarse si esta divulgación, transferencia o utilización no se corresponde con el fin especificado en el momento de la recogida de los datos. Las

excepciones a este principio son posibles con el consentimiento del interesado o si la utilización tiene lugar en el marco de una imposición legal.

La falta de un fin inicial específico impide también el principio de limitación de uso y hace que resulte imposible imponer ningún límite en relación con usos secundarios. Asimismo, la vinculación espontánea de innumerables ordenadores invisibles y el intercambio de datos entre ellos representa un componente básico e indispensable de las infraestructuras de computación ubicua; por lo tanto, existe una contradicción obvia y fundamental entre los principios de limitación de uso y especificación de propósito y las visiones de los sistemas de computación ubicua.

Todos los intentos de hacer cumplir partes de este principio también implicarían la reducción de los beneficios potenciales y la posibilidad de uso de las infraestructuras de computación ubicua. La capacidad de utilización queda restringida porque la consulta permanente acerca del consentimiento o la oposición a solicitudes de transferencia de datos se opondría a la intención de crear entornos de computación discretos y seguramente exasperaría a cualquier usuario en un breve periodo de tiempo.

3.3.5 Principios de procedimiento

Los últimos cuatro principios describen principalmente políticas y aspectos técnicos y de procedimiento necesarios para hacer cumplir y proteger el cumplimiento de los primeros cuatro principios. También proporcionan transparencia y establecen los derechos de los interesados individuales a ser informados y a cuestionar los datos relativos a ellos. Varias contradicciones entre el concepto de computación ubicua y estos principios restringen o eliminan su aplicabilidad bajo el nuevo paradigma de tecnología.

Resultará prácticamente imposible proporcionar niveles suficientes de seguridad contra acceso no autorizado o divulgación de datos cuando el establecimiento de conexiones espontáneas de numerosos componentes inalámbricos con capacidades de cifrado y tratamiento limitadas supone un elemento básico de dichos sistemas.

El objetivo general del Principio de Transparencia puede tenerse en cuenta informando acerca de la presencia de tecnologías de computación ubicua; los requisitos específicos como la información acerca de la naturaleza de los datos personales o de su objetivo principal no pueden cumplirse a causa de la recogida de datos dinámica y de la falta de objetivos específicos previos.

Dependiendo de la aplicación concreta de los sistemas de computación ubicua, puede resultar difícil o imposible identificar al responsable(s) de tratamiento responsable, según requiere el último punto de las Directrices de la OCDE, el Principio de Responsabilidad.

3.3.6 Decisiones automatizadas de las personas

La Directiva de Protección de Datos contiene otra disposición que contradice de forma evidente los mecanismos de toma de decisiones y de prestación de servicios previstos basados en la creación de perfiles de computación ubicua, puesto que indica «…reconocerán a las personas el derecho a no verse sometidas a una decisión con efectos jurídicos sobre ellas o que les afecte de manera significativa, que se base únicamente en un tratamiento automatizado de datos destinado a evaluar determinados aspectos de su personalidad, como su rendimiento laboral, crédito, fiabilidad, conducta, etc.». «Esta prohibición parece enfrentarse, asimismo, a la lógica de la creación de perfiles autónomos adaptativos, […], puesto que la mayoría de las decisiones las tomarán máquinas en un proceso de comunicación de máquina a máquina».

3.4 Propuestas para superar las contradicciones

El progreso técnico de las tecnologías de la información y de la comunicación, las nuevas formas de prestación de servicios o la aparición de formas innovadoras de utilizar plataformas técnicas, crean con frecuencia nuevos problemas y requieren nuevas normativas o nuevas o ampliadas interpretaciones de las existentes.

Las contradicciones con los principios de limitación de recogida y de especificación de propósito corresponden a las debilidades más graves y

urgentes de los marcos actuales de protección de la privacidad cuando se aplican al nuevo paradigma tecnológico. Obviamente, la minimización de la generación y recogida de datos personales ya resulta hoy en día cada vez más difícil de aplicar; en entornos de computación ubicua, este esfuerzo se convertirá en un concepto inútil y sin sentido.

Por consiguiente, la atención reguladora podría trasladarse a la utilización con respecto a la prevención del abuso de datos personales o del conocimiento obtenido a partir de éstos. Este enfoque requeriría volver a conceptualizar la privacidad en lo que respecta al acceso al conocimiento en lugar de los datos y a la protección contra una utilización injusta de este conocimiento.

La aplicabilidad y eficacia de dicha reforma normativa dependerá básicamente de la capacidad de incrementar la transparencia del tratamiento, del análisis y de las transferencias de los datos; existen pocos motivos para el optimismo, teniendo en cuenta la asimetría cada vez mayor de la información y la complejidad de las tecnologías de computación ubicua.

La única disposición aplicable en este contexto, el artículo 15 sobre decisiones individuales automatizadas de la Directiva 95/46/CE, no proporciona una protección suficiente para los ciudadanos contra esta práctica.

El incremento de la transparencia[352] del tratamiento de datos y de la utilización de la información generada a partir de este tratamiento constituye

---

[352] Con el fin de hacer un consentimiento realmente informado, se elaborarán políticas transparentes y fácilmente accesibles por lo que respecta al tratamiento de datos personales y al ejercicio de los derechos de los interesados. Estas políticas deben ser elaboradas de forma concisa, transparente, inteligible, y de fácil acceso, con un lenguaje sencillo y claro, especialmente si los interesados son menores [Vid el artículo 12.1 RGPD]. Este principio afectará al principio de información. Transparencia e información son requisitos que deben ir de la mano en cualquier sociedad democrática. La información de quién, por qué y para qué se tratan los datos personales se vuelve más transparente. Se propone por parte del RGPD una normalización de las políticas de información. Así, ésta se podrá llevar a cabo a través de un conjunto de iconos gráficos, que se utilizarán por parte del responsable del tratamiento antes de informar [Vid. Considerando 60 y artículo 12.7 RGPD]. En realidad, se facilita a los responsables del tratamiento el cumplimiento con sus obligaciones, propiciando que las «políticas de privacidad» o «el deber de información» se cumplan de una manera

un requisito previo para concebir beneficios resultantes del cambio sugerido en el centro de atención de la regulación y la limitación de la recogida de datos a la utilización del conocimiento. De acuerdo con ello, las herramientas de transparencia se consideran un elemento clave de marcos jurídicos futuros capaces de limitar las amenazas a la privacidad de la computación ubicua. Sin embargo, resulta bastante cuestionable el grado en el que la transparencia puede desempeñar el papel clave atribuido bajo el nuevo paradigma de tecnologías de la información. Una mayor transparencia, especialmente en entornos de computación ubicua, contradiría el objetivo de la discreción. Asimismo, la transparencia no resulta suficiente para crear libertad de elección para los interesados, en general, con respecto al uso que puede darse a los datos y al conocimiento obtenido; puede mejorar la simetría de la información, pero no puede eliminar las asimetrías de poder. La transferencia del tratamiento de esta información y la toma de decisiones posterior a los asistentes digitales personales o agentes se encuentra asociada a una transferencia correspondiente de autonomía individual; asimismo, las preferencias de privacidad requeridas para el funcionamiento de estos agentes constituyen por sí mismas datos personales de una naturaleza potencialmente muy sensible.

Las normativas existentes, ancladas en los principios de minimización y especificación de fines o el requisito de consentimiento relacionado con la recogida de datos ya no resultan aplicables bajo el nuevo paradigma tecnológico, deben complementarse mediante disposiciones que limiten el

---

más eficaz, siendo más accesibles con un lenguaje visible, claro y sencillo. El problema lo vamos a encontrar en las dificultades técnicas que se producen cuando el tratamiento de datos se produce en Internet, pues en la mayoría de las ocasiones tendremos dificultades para conocer quién puede haber llevado a cabo un tratamiento de datos, lo que complica no solo el deber de informar, sino, en último término, el ejercicio de los derechos [Valero Torrijos, J. (2013). Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado. En Valero Torrijos, J. (Coord..). *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Navarra: Aranzadi, p. 57]. Con estas medidas se logra reforzar el carácter informado del consentimiento, convirtiéndolo en una obligación propia de un estándar internacional [La «Resolución de Madrid» reconoce el principio de transparencia en su apartado 10]. Y reforzando el consentimiento, reforzamos el control de nuestros datos personales.

uso y protejan contra el abuso del conocimiento generado. En principio, resulta necesario y positivo imponer restricciones normativas al tratamiento y a la utilización de datos generados por infraestructuras de computación ubicua; sin embargo, puede resultar muy difícil controlar y cumplir dichas restricciones debido a la naturaleza ubicua aunque invisible de esta tecnología. Por supuesto, resultará necesario respetar los principios relacionados con la privacidad desde el diseño[353], y la privacidad por

[353] Aunque nos referiremos a esta medida con posterioridad, indicar que el concepto de Privacy by Design supone una garantía adicional al tratamiento de datos personales al recoger la obligación del responsable de desarrollar las medidas de protección –tanto técnicas como organizativas– de dichos datos, con carácter previo al tratamiento de datos personales que se quiera realizar [Artículo 25.1 RGPD Protección de datos desde el diseño y por defecto «1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados»]. Se aplica a servicios y productos, por lo que se tendrá en cuenta, también, el principio de minimización de datos (Privacy by default) y el de finalidad de los mismos. Este tipo de medida se basa en siete principios fundamentales que vienen siendo promovidos por las Autoridades de Protección de Datos desde el año 2010 con el fin de garantizar y fomentar la privacidad de y entre los ciudadanos [Véase la Resolución sobre Privacidad desde el Diseño (2010). XXXII Conferencia Internacional de Autoridades de Protección de Datos, de 27-29 de octubre de 2010. En https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf]. Estos principios son: i) Principio proactivo no reactivo y preventivo no correctivo; ii) Privacidad como la configuración predeterminada; iii) Privacidad incrustada en el diseño; iv) Funcionalidad total, «todos ganan», no «si alguien gana, otro pierde»; v) Seguridad extremo a extremo, protección de ciclo de vida competo; vi) Visibilidad y transparencia (mantenerlo abierto); y, vii) Respeto por la privacidad de los usuarios, mantener un enfoque centrado en el usuario [Se pueden consultar en Cavoukian, A. (2011). Privacy by Design. Los 7 principios fundamentales. Recuperado de https://www.acc.com/chapters/euro/upload/7foundationalprinciples-spanish.pdf]. No obstante, esta nueva obligación se hace depender de la tecnología existente, así como del coste de implementación que le suponga al responsable [Véase Rubí Navarrete, J. (2013). La propuesta del Reglamento General de Protección de Datos de la Unión Europea. En *Comunicaciones e propiedad industrial y derecho de la competencia, 70*, p. 122. Se ha calificado esta obligación como «una obligación de naturaleza dinámica que deberá ir adaptándose a la evolución de la tecnología y de sus costes»]. El peligro es evidente, pues se hacen depender las medidas de seguridad a implantar de la ponderación que al respecto realice el responsable del tratamiento.

defecto[354], para de este modo, añadir tecnologías de protección de la privacidad cuando sea posible.

[354] De igual modo, y aunque nos referiremos a esta medida con posterioridad, indicar que el concepto de Privacy by Default viene a reforzar el actual principio de calidad de los datos conforme al cual, los datos para su tratamiento deben ser adecuados, pertinentes y no excesivos. En este sentido, el RGPD se refiere a la necesidad de adopción de medidas de protección de datos, de carácter técnico u organizativo, por defecto, Privacy by default [Artículo 25.2 RGPD Protección de datos desde el diseño y por defecto «2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas»]. Esto es, que por defecto se minimice el número de datos personales tratados, así como que su conservación se realice estrictamente, en función de la finalidad de tratamiento. En el sector privado, esto significaría una menos probabilidad de fallos o brechas de seguridad y, por lo tanto, supondría una mejor garantía del derecho a la protección de datos personales de los ciudadanos. La idea es que esos mecanismos garanticen que, por defecto, el número de personas que pueden acceder a ellos no sean indeterminados y que los titulares de los datos sean capaces de controlar la distribución de los mismos. Asimismo, la promoción de este principio en el uso de las redes sociales, evitaría que fuera el usuario el que tuviera que elegir las medidas de privacidad, que vendría configurada por defecto y evitaría los habituales problemas que se producen de cesiones de datos sin consentimiento de sus usuarios [Troncoso Reigada, A. (2012). Hacia un nuevo marco jurídico europeo de la protección de datos personales. *Revista Española de Derecho Europeo, 43*, *pp. 51-52*].

CAPÍTULO IIIº: LA TRANSPARENCIA

SUMARIO: 1. NOTAS SOBRE EL DERECHO ADMINISTRATIVO DE LA INFORMACIÓN. 1.1. Concepto de transparencia. 1.2. El principio democrático y la buena administración. 1.3. Aproximación al derecho a la información administrativa en la legislación norteamericana. 1.4. El impulso del Derecho Comunitario a la publicidad y transparencia de la Administración. 1.5. La evolución en la relación de los derechos de protección de datos de carácter personal y de acceso a la información pública en el ámbito de la Unión Europea. 1.6. Los esperables efectos de la nueva regulación en el ámbito comunitario. 1.7. Desarrollo del principio de transparencia a través de la jurisprudencia del Tribunal de Justicia. 1.8. Incidencia del Reglamento en las relaciones entre el derecho de acceso a la información y el derecho a la protección de datos de carácter personal en el ámbito interno español. 2. EL DERECHO A LA INFORMACIÓN, LA PUBLICIDAD Y TRANSPARENCIA EN LAS RELACIONES ENTRE LA ADMINISTRACIÓN, EL CIUDADANO Y EL PÚBLICO. 2.1. Introducción. 2.2. Derecho a la información y cuentas públicas. 2.3. La relación entre la publicidad y el principio de transparencia en la actuación de la Administración. 3. LA EXIGENCIA DE UNA ADMINISTRACIÓN TRANSPARENTE EN LA PERSPECTIVA DEL ESTADO DE DERECHO. 3.1. Aparición y difusión de la transparencia como principio rector de la modernización del Estado. 3.2. Las funciones de la transparencia administrativa. 3.3. Sujetos obligados y derecho de acceso. 3.4. Concepto de información pública. 3.5. La naturaleza jurídica del Derecho de Acceso y el conflicto con otros derechos e intereses. 3.6. Los límites del derecho de acceso a la información pública. 4. EFECTIVIDAD DE LA TRANSPARENCIA: PUBLICIDAD ACTIVA Y PUBLICIDAD PASIVA. 4.1. Publicidad Activa. 4.2. El derecho de acceso a la información. Publicidad pasiva.

1 NOTAS SOBRE EL DERECHO ADMINISTRATIVO DE LA INFORMACIÓN

1.1 Concepto de transparencia.

El concepto de transparencia no es unívoco, pues tiene carácter poliédrico con múltiples formas y que puede diferenciarse entre una transparencia en la decisión, en el procedimiento, en el contenido de la norma y en la responsabilidad. Ni siquiera esta descripción agota su significado porque únicamente refleja su contenido procedimental[355].

[355] Sommermann, K. P. (2010). La exigencia de una Administración transparente en la perspectiva de los principios de democracia y del Estado de Derecho. En García Macho, R. (Ed.), *Derecho administrativo de la información y administración transparente*. Madrid: Marcial Pons, p. 11.

Transparencia también es control, que puede y debe ser realizado por los órganos del Estado que tienen como función propia su ejercicio sino también por la ciudadanía a través de la participación.

A su vez, este control ciudadano puede ser realizado con anterioridad a la toma de decisión y/o, posteriormente, por lo que la transparencia también se encuentra directamente asociada con la rendición de cuentas que todo gobierno debe realizar en razón del manejo que realiza de la cosa pública.

Si la transparencia es un concepto que se subsume en el Estado de Derecho y donde el ciudadano toma conocimiento de las razones que llevan al gobernante a adoptar determinada acción, en los términos que se indicarán más adelante, la propia realización del Estado de Derecho exige que, en forma primaria, el gobernante tenga una obligación jurídica de informar al ciudadano, y éste, el derecho a tener conocimiento de la cosa pública.

Por ello, en los Tratados de Derechos Humanos la transparencia se encuentra íntimamente vinculada con el derecho a la información pues sin transparencia no podría afirmarse que este derecho pudiera existir y viceversa, sin el derecho a la información, la transparencia tampoco existiría.

El derecho al conocimiento de la actividad del Estado y, concordantemente, el derecho a ser informado, permiten sostener una relación adecuada entre el gobernante y el ciudadano.

Dentro de este contexto, en el Derecho comparado se observa una ampliación gradual de los derechos de los particulares a efectos de exigir al Estado la publicidad de sus actos, de tal manera que la actividad sea realizada son ocultamiento alguno, es decir, sea transparente[356].

---

[356] Se ha expresado que «la transparencia es la posibilidad de conocer información veraz, completa y oportuna sobre la forma en la que manejan los recursos públicos, la cual deberá estar expuesta de forma permanente en medios remotos, preferiblemente electrónicos», Pulido Jiménez, M. Á. (2006). Una aproximación a la información pública en poder de la CNDH. El acceso a la información en la CNDH. En A. Ruiz Euler (Coord.), *Transparencia y Rendición de Cuentas*. México DF: Fontamara. p. 110.

Por esto puede decirse que a mayor respeto del derecho de información el Estado actúa con mayor transparencia y este es uno de los caminos que conducen al fortalecimiento de la democracia. Porque la existencia del secreto en la actuación de la Administración impide tener conocimiento de la génesis de sus decisiones, y da un mayor poder a quien así lo practica. Por el contrario la transparencia permite el acceso a las fuentes mismas del proceso de decisiones, permitiendo la participación informada a los ciudadanos, a partir de dicho conocimiento, intervenir o ejercer los instrumentos de control sobres las decisiones jurídicas de la Administración pública.

Se permite que aquellos no solo conozcan la actividad de la misma, sino que puedan emitir opiniones sobre las decisiones y el que la adopta, al encontrarse visualizado necesariamente deberá hacerse responsable de su actuar[357].

Por tanto, la transparencia es un principio que guía a la buena Administración en un Estado de Derecho. Es la materialización del derecho al conocimiento: la manera de ejercitarlo es asegurar los mecanismos procesales para que se cumpla con el derecho a la información.

El principio de transparencia dispone que, frente a una actividad gubernamental, ya sea activa o pasiva, es necesario que se publicite la misma de tal manera que no se practique en secreto, siempre y cuando no existan limitaciones legales para tener acceso a la documentación correspondiente[358].

La transparencia se entiende como un fin que tiene un significado cualitativo en una democracia y que remite a la idea de publicidad. Publicidad

---

[357] «La transparencia debe ser una regla para ser y comportarse, parámetro que guía la actuación administrativa que, al igual que la eficiencia y la objetividad, debe determinar su comportamiento». Blasco Díaz, J. L. (2010). El sentido de la transparencia administrativa y su concreción legislativa. En García Macho. R. (ed.), *Derecho administrativo dela información y administración transparente*. Madrid: Marcial Pons, p. 128.

[358] Basterra, M. I. (2006) *El Derecho Fundamental de Acceso a la Información Pública*. Buenos Aires: Lexis Nexis, p. 30.

entendida como posibilidad de conocimiento de la información, frente a la idea de secreto, lo que remite a su vez a la idea de responsabilidad de los poderes frente a la ciudadanía.

La transparencia como principio exigiría que el acceso a la información no requiriera tener la condición de interesado. Para ello, debe ser ejercitado sin que haya necesidad de justificar un determinado interés. El mismo es propiedad de la ciudadanía. Si el acceso es consecuencia de la transparencia en el funcionamiento de los poderes públicos, ese acceso tendría que ser independiente e indiferente al interés de la persona solicitante. Tampoco tendría que estar limitado a determinadas asociaciones o defensores de intereses colectivos o difusos. En los ámbitos materiales en que esté prevista la acción pública tampoco habrá lugar a la negación del acceso por no tener la condición de interesado.

1.2 El principio democrático y la buena administración

El fundamento constitucional de la transparencia se sustenta en el principio que caracteriza al poder público en un Estado democrático, que se proyecta sobre la actividad de su Administración. El conocimiento de la gestión pública, y por ello, de la utilización de los fondos públicos, permite la participación ciudadana como el ejercicio de su derecho de decisión democrática por los actores.

En ambos supuestos, la trasparencia se vincula al principio democrático, pues asegura un control democrático del poder, y por ello de la actividad administrativa, de su desarrollo y adecuación con el interés público, al tiempo que permite a la ciudadanía contrastarla con sus expectativas o criterios.

En consecuencia, puede entenderse que los poderes públicos deben suministrar a los ciudadanos toda aquella información que les permita conocer y valorar lo realizado por quienes los representan o, cuanto menos, susceptible de ser conocidas por aquéllos. Se deben conocer tanto las decisiones políticas adoptadas y por qué se han adoptado, como las decisiones administrativas y económicas, es decir, por qué se ha decidido

algo y cómo se han utilizado los recursos públicos o se van utilizar, despejando asimismo su preocupación de que no se actúa al servicio de intereses particulares. Y ello debe realizarse en todos los ámbitos del poder público.

En las democracias puede considerarse que con ello se refuerza la legitimidad de las instituciones. De este modo, se ha entendido que el derecho a acceder encontraría su fundamento en el denominado «aspecto crítico» del principio democrático, que constituye a su vez una de las dimensiones básicas del estatuto de la ciudadanía, o lo que es lo mismo, de «democracia abierta», que, sin excluir la democracia jerárquica, va más allá y parte de presupuestos más activos de democracia, en los que se considera que la participación directa de la sociedad civil en el proceso de formación de la voluntad política no es discordante, sino contrariamente es un efecto del proceso democrático y del principio democrático .

En este sentido, el Tribunal Supremo, en su Sentencia de 16 de febrero de 2004, señala que, «cuando el artículo 3. núm. 5 de la Ley de Régimen Jurídico de las Administraciones públicas y del Procedimiento administrativo común proclama que la Administración actuará en relación con los ciudadanos conforme al principio de transparencia, no está haciendo una hueca proclama populista, sino incorporando al Derecho positivo un principio sustentador de un Estado, como lo es el Estado español, que no solo es social y democrático sino también de Derecho. Porque uno de los rasgos definidores —no meramente retórico— de la democracia es el de que en un Estado de ese tipo, los poderes públicos —todos ellos, por supuesto el judicial hablando por medio de sus sentencias y resoluciones, pero también los demás, y por tanto la Administración pública— han de dar razón de sus actos, lo que quiere decir que han de explicar razonada y razonablemente el porqué de sus decisiones».

En definitiva, el vínculo de la transparencia con el principio democrático se manifiesta en una doble vertiente, por un lado, aquella es consustancial al funcionamiento democrático de un Estado, por otro también es instrumental para que el ejercicio de la democracia por los ciudadanos se pueda realizar con el adecuado conocimiento de cuanto les concierne. Se constituye así en

una pieza necesaria para ejercer la facultad de decidir, de participar en los asuntos públicos a través del control democrático del artículo 23.1 de la Constitución. De igual modo, con transparencia se facilita la participación de todos los ciudadanos en la vida política, económica, cultural y social, tarea que el artículo 9.2 de la Constitución encomienda a los poderes públicos. Participación que deviene en imposible si no se cuenta con los elementos necesarios, con la información indispensable para que pueda ser efectiva y real.

Si una finalidad de la transparencia es que esos actos y sus consecuencias deban ser conocidos por la sociedad, otra de sus virtualidades es la de posibilitar un control de la actividad pública, más allá del de tipo democrático. Es decir, un control tanto de carácter económico-financiero, como, eventualmente, en sede judicial, perspectiva desde la que aquella se contempla como un instrumento de garantía de la legalidad, la eficacia y la objetividad de la Administración. De este modo, se posibilita poder actuar tanto frente a situaciones en las que se afecta negativamente al buen gobierno, como ante las situaciones de corrupción o mala praxis.

También es cierto que la contabilidad no asegura la transparencia de por sí, sino que su utilidad es la de crear los datos cuya publicidad permite garantizar la transparencia, es decir, el sistema contable no proporciona en realidad ninguna transparencia, sino que constituye un presupuesto para que sea posible asegurar, mediante la publicidad de las cuentas o el acceso a ellas, transparencia acerca de la recepción y el empleo de los recursos del ente.

Por último, se revela también de una trascendental importancia en este aspecto, el papel que deben desempeñar tanto los medios de comunicación social como las organizaciones y entidades en las que pueden integrarse los ciudadanos, así como las formaciones políticas, sujetos todos ellos más capacitados con carácter general para conocer, comprender y tratar la información ofrecida y, por ello, poder actuar en consecuencia, bien sea difundiéndola de un modo accesible para el resto de la sociedad o emprendiendo las actuaciones necesarias para depurar responsabilidades y

enmendar posibles irregularidades que hayan podido incurrir las actuaciones conocidas.

1.3 Aproximación al derecho a la información administrativa en la legislación norteamericana

La Constitución de este país no establece un derecho explícito al acceso a la información, sino que la tenue existencia del mismo depende de una construcción jurisprudencial basada en la primera enmienda a la misma. La legislación estadounidense ha ido construyendo un acervo normativo sobre el derecho a la información que obra en manos de los poderes públicos que, en su día, fue pionero y que en muchos aspectos ha servido de base a las normas introducidas en otros países.

La primera norma de la legislación norteamericana relacionada con el derecho a la información administrativa, se denomina The Adminsitrative Procedure Act, aprobada en 1946[359]. Esta ley recoge la filosofía del Derecho administrativo americano prevalente en aquella época, posibilitando el acceso a los archivos administrativos solamente a aquellas personas «con un interés legítimo y directo», lo cual dejaba en manos de la Administración un amplio margen de discrecionalidad.

En los años cincuenta la doctrina empezó a cuestionar la interpretación restrictiva que se daba al acceso a la información administrativa, dando lugar a que en 1955 el Congreso iniciara un proceso para reformarla, que desembocó en la aprobación de The Freedom of Information Act en 1966. Esta ley sentó los principios que todavía se aplican en buena medida a la información administrativa, estableciendo un derecho presunto a disponer de la información existente e identificable en posesión de las Agencias administrativas federales, fijando dos categorías de información. En primer lugar, aquella información que se tenía que facilitar de forma automática y,

[359] Admisnitrative Procedure Act – 5 USC Subchapter II

en segundo lugar, otra información que quedaba sujeta a nuevas exenciones específicas, como la seguridad nacional y el secreto comercial, entre otras.

En este proceso de reforma hacia un mayor derecho a la información administrativa debemos destacar dos leyes relevantes, The Federal Advisory Committe Act, de 1972[360], y The Government in the Sunshine Act, de 1976[361].

De igual modo, debemos mencionar The Privacy Act, de 1974[362], que introdujo un régimen que aún se aplica en Estados Unidos en cuanto a la protección de datos personales en aras a la preservación de la intimidad personal, incidiendo directamente sobre el derecho a la información, protegiendo al ciudadano frente a la difusión de la información por parte de la administración perteneciente a su ámbito privado, e imponiendo restricciones sobre la forma en la cual la Administración federal puede obtener, utilizar y difundir la información personal.

La norma de aplicación ante las solicitudes de acceso a la información es la Freedom of Information Act (FOIA) y no la Privacy Act, que se remite a ésta. La FOIA contempla una excepción a la divulgación de información administrativa en razón de la protección de la privacidad, que llama a una ponderación entre este derecho y el interés público general en el conocimiento de información directamente relacionada con el funcionamiento y control de la Administración. Se sigue un sistema de Autoridad única: una misma Institución, la Office of Information and Privacy (OIP), vigila por la correcta aplicación de la FOIA y su coordinación con la Privacy Act[363].

---

[360] Federal Advisory Committee Act – 5 USC Appendix 2.

[361] Government in the Sunshine Act of 1976 – 5 U.S.C. § 552b.

[362] Privacy Act of 1974, 5 U.S.C. § 552a.

[363] Para la aplicación de la FOIA se creó, en el seno del Departamento de Justicia, la Office of Information and Privacy (OIP), que es la responsable de supervisar el cumplimiento de la FOIA por parte de la Administración Federal a la que asesora sobre esta materia. La Privacy Act de 1974 (5.

Al regular las condiciones de divulgación de datos personales en poder de la Administración federal, esa prohíbe con carácter general la misma salvo con el consentimiento del afectado o en los casos previstos en la propia norma, entre los cuales se encuentra precisamente el supuesto en que se requiera el acceso conforme a la FOIA. El principio es, pues, que la Privacy Act nunca prohíbe una divulgación que viene requerida en aplicación de la FOIA[364]. De esta forma, si ha de concederse el acceso conforme a la FOIA, se procede al mismo. Si, por el contrario, concurre la excepción de la protección de la privacidad contemplada en la FOIA, la Privacy Act prohíbe la divulgación de la información, dado que sólo prevé la divulgación cuando la misma es requerida por la FOIA, esto es, no la somete a las consideraciones de apreciación discrecional propias de la FOIA[365]

El derecho de los ciudadanos a acceder a la información en poder de la Administración federal se regula en la Freedom of Information Act de 1966, que fue uno de los textos pioneros a nivel mundial en el reconocimiento del derecho de acceso a la información pública, y ha sido objeto de sucesivas reformas[366]. Se trata de una Ley avanzada tanto en sus aspectos sustantivos[367] como en los procedimentales[368]. Esta norma contempla una

---

U. S. C. 552 a) es la norma que regula el derecho a la protección de datos frente a la Administración federal.

364 Véase Greentree v. United States Customs Serv., 674 F.2d 74, p. 79 (D. C. Cir. 1982), conforme a la cual esta previsión representa un mandato del legislador para que la Privacy Act no se utilice como barrera al acceso conforme a la FOIA.

365 Por todos, Sentencia Tribunal Supremo de los Estados Unidos. United States Department of Defense v. Federal Labor Relations Authority, [510 U. S. 487, (1994)].

366 Entre las diferentes reformas que han ido operándose en el texto original, la principal fue la llevada a cabo en 1996 por las Electronic Freedom of Information Act Amendments, que supuso su adaptación a la era digital.

367 Establece no sólo el derecho de acceso a instancia de cualquier ciudadano sino toda una serie de obligaciones precisas en orden a la gestión de la información y la puesta en disposición de todos los ciudadanos, sin necesidad de solicitud, en papel y en formato electrónico, de la información más relevante para el conocimiento y control de la actividad del ejecutivo, así como la existencia de un registro de libre consulta que clasifica esta información.

368 El procedimiento de información a solicitud de un ciudadano es ágil, con un plazo de resolución de veinte días –anteriormente diez–, que puede ampliarse en casos excepcionales, que se tramita por

serie de excepciones que *pueden* ser apreciadas por la Administración[369], entre las que se encuentran los ficheros de personal o médicos y ficheros similares cuya divulgación constituiría una invasión claramente injustificada de la privacidad personal[370]

En síntesis, en el Derecho federal estadounidense, las relaciones entre privacidad y publicidad están reguladas en la normativa sobre acceso a la información a la que se remite expresamente la ley reguladora del derecho a la privacidad. Una Autoridad única vela por la armonización de ambos derechos y la coordinación en la aplicación de ambos grupos normativos. El principio general es el de ponderación entre el respeto a la privacidad y el interés público general en el conocimiento de información directamente relacionada con el funcionamiento y control de la Administración. Es este último, y no el acceso "instrumental" a la informació para la tutela de derechos o intereses particulares, el que protege la normativa sobre acceso, lo que lleva a que el juicio ponderativo sea de carácter objetivo, esto es, basado en la relevancia pública de la información, con desvinculación del interés concreto del solicitante. Esto explica que en la ponderación prevalezca la publicidad de la información más directamente relacionada con la necesidad de control y transparencia de la actuación administrativa,

---

la autoridad que detenta la información, contra cuya decisión cabe apelar ante el director de la respectiva agencia y ulterior recurso judicial. En caso de silencio, cabe acudir directamente ante los tribunales.

[369] En su sección b). Así, las relacionadas con los documentos clasificados por razones de defensa y política exterior; normas y prácticas internas en materia de personal; expresamente excluidos de publicidad por ley; secretos comerciales e información comercial o financiera obtenidas con carácter confidencial; cartas o *memorandums* inter o intraadmnistrativos que conforme a la ley sólo deban estar a disposición de las agencias; información relacionada con los procedimientos en materia de orden y seguridad pública (law enforcement), en determinadas condiciones; o en materia de regulación o supervisión de las instituciones financieras; o informaciones y datos geológicos o geofísicos, incluidos los mapas, referida a bienes.

[370] En el caso de la información relacionada con los procedimientos en materia de seguridad pública, se prevé específicamente entre las excepciones al libre acceso el caso en que pueda esperarse razonablemente que constituya una invasión injustificada de la privacidad personal.

mientras que prepondera el derecho a la privacidad en todos los datos personales cuyo conocimiento es innecesario para dicho objetivo.

Estas cuatro Leyes han sentado las bases de una política de acceso a la información administrativa impregnada de una filosofía basada en una presunción de que la participación de la ciudadanía en el proceso democrático fortalecía a la sociedad americana, y que el acceso a la información que obrara en manos de las Administraciones Públicas es un pilar esencial en que se apoya dicha participación.

1.3.1 Regulación constitucional

En la Constitución norteamericana, a diferencia de algunos textos constitucionales más recientes, no existe una referencia explícita al derecho de acceso a la información administrativa. Sin embargo, se ha querido postular la existencia de este derecho estableciendo una relación entre el derecho a la liberta de expresión, el derecho a informar, el derecho a ser informado y, finalmente, el derecho a acceder a la información del gobierno.

La primera enmienda de la Constitución establece:

> *«Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances».*

«El Congreso no aprobará ninguna ley […] que coarte la libertad de expresión o de prensa». De aquí se ha querido postular un derecho a transmitir la información, de libre expresión, que acarrea también un derecho incorporado a recibir información. En la construcción del posible derecho a acceder a la información, la doctrina ha querido extender el derecho a ser informado para incorporar un derecho que es el de recibir una información veraz. Es partiendo de aquí de donde se ha querido construir un derecho de acceso a la información, que se supone será más fuerte en el caso de la información que obre en manos de la Administración, dada la posición de la Administración como «servidora del pueblo».

La redacción de la enmienda parece otorgar una posición privilegiada a los medios de comunicación y una mayor protección de su derecho a expresarse. Sin embargo, el Tribunal Supremo ha otorgado más protección al derecho a recibir información que al derecho a acceder a ella[371]. Ha sido en el ámbito legislativo donde se han tenido que construir los principios aplicables al derecho a la información, y la legislación estadounidense ha ido construyendo un acervo normativo sobre el acceso a la información que obra en manos de los poderes públicos que, en su día, fue pionero, y que en muchos aspectos ha servido de base a normas similares introducidas en otros países.

1.3.2 La regulación del derecho de acceso a la información administrativa en la legislación ordinaria

1.3.2.1 The Freedom of Information Act

El proceso de reforma de la *Administrative Procedure Act* desembocó en la aprobación de *The Freedom of Information Act.* Esta ley sentó los principios que todavía se aplican en buena medida a la información administrativa, estableciendo un derecho presunto a disponer de la información existente e identificable en posesión de las Agencias administrativas federales, fijando dos categorías de información.

En primer lugar, aquella información que se tenía que facilitar de forma automática y, en segundo lugar, otra información que quedaba sujeta a nueve exenciones. El acceso a la información no se restringía a los

---

[371] El caso más importante en esta materia ha sido el caso Houchins vs. KQED, [Houchins vs. KQED, Inc., 438 US 1 (1978)]. El Tribunal Supremo no solo decidió que no existe un derecho preferente de los medios de comunicación a acceder a la información de la Administración, sino que tal derecho constitucional de acceso a la información administrativa no existe como tal. Para el Tribunal, la Constitución no garantiza al público un derecho de acceso a la información generada por y controlada por la Administración, sino que lo único que garantiza la Constitución es la igualdad de acceso a la información que quiera proporcionar la Administración. Para el Tribunal, aunque no se dude de la existencia de un derecho de recabar información mediante cualquier método legal, este derecho no presupone base alguna para entender que la primera enmienda obliga a otras, personas privadas o a la Administración, a proporcionar dicha información.

«interesados», sino que establecía un derecho presunto para que «cualquier persona física o jurídica» tuviera acceso a la información administrativa existente, no publicada, sin tener que alegar un interés específico, con las únicas limitaciones de las nueve exenciones anteriormente mencionadas.

El Tribunal Supremo declaró expresamente en el caso *Favish*[372] que «cuando un documento queda sujeto a las previsiones de *The freedom of Information* no se debe obligar al ciudadano a explicar por qué quiere la información. De hecho, una persona que solicita la información no necesita saber por qué la quiere. La información es propiedad del ciudadano y puede hacer con ella lo que quiera. Además, la divulgación de la información no depende de la identidad del solicitante. Como regla general, si la información está sujeta a las previsiones de la ley, es propiedad de todos».

Existen dos categorías de información: i) información que debe facilitarse «automáticamente». Este tipo de información se encuentra detallada en la ley, e incluye reglamentos, documentos sobre la organización de las Agencias administrativas y opiniones sustantivas de las mismas; y, ii) información administrativa cuya puesta a disposición del ciudadano requiere de una solicitud por parte del ciudadano y una respuesta de la Administración que tiene en cuenta si es factible el recabar la información, y una decisión sobre si la información recae dentro de las exenciones contenidas en The Freedom of Information Act.

1.3.2.1.1 Exenciones a The Freedom of Information Act

El legislador no ha querido dar un alcance ilimitado a la ley, autorizando la divulgación de cualquier información administrativa a cualquier persona. No obstante, los Tribunales han interpretado estas exclusiones teniendo en cuenta el espíritu de apertura democrática de la Ley. Así, las exenciones son:

---

[372] Sentencia Tribunal Supremo de los Estados Unidos de 30 de marzo de 2004, National Archives and Records admin. vs. Favish, [541 US 157 (2004)].

1) Información cuyo carácter secreto se establece de forma específica siguiendo los criterios incluidos en una *Presidential Executive Order*, en aras a la defensa de la nación o la política exterior, y que ha sido efectivamente clasificada según lo dispuesto en dicha *Executive Order*.

Información referente únicamente a las normas internas relativas a las normas sobre el personal de la Agencia y jsobre sus prácticas internas.

Información exenta según las previsiones de otra ley, siempre y cuando dicha ley prohíba su divulgación de tal forma que no se permita ninguna interpretación discrecional.

Información clasificada como secretos comerciales e información comercial o financiera obtenida de una persona que se considera privilegiada o confidencial.

Memorándums o cartas interadministrativas o intra-administrativas. No se facilitarán a ninguna persona salvo cuando una Administración se encuentra inmersa en un proceso judicial contra otra Administración.

Información incluida en los Archivos de personal o archivos médicos y similares, cuya divulgación supondría un ataque claramente injustificado a la intimidad personal.

Archivos y registros o información reunidos con fines de hacer cumplir la ley

Asuntos contenidos en o relacionados con informes preparados directamente por, o por encargo de, una Agencia responsable de la regulación o supervisión de instituciones financieras.

En 1974, The Privacy Act introdujo un régimen que aún se aplica en los Estados Unidos en cuanto a la protección de datos personales en aras a la preservación de la intimidad personal, incidiendo directamente sobre el derecho a la información, protegiendo al ciudadano frente a la difusión de la información por parte de la Administración perteneciente a su ámbito privado e imponiendo restricciones sobre la forma en la cual la Administración federal puede obtener, utilizar y difundir la información personal.

En aras a una mayor eficacia, The Freedom of Information Act de 1996 ha sido enmendada en varias ocasiones antes de que se aprobase The Electronic Freedom of Information Act.

Hasta este momento, el suministro de la información obrante en manos de la Administración se había entendido como una obligación que se debía cumplir solo en el momento de recibir una solicitud realizada por un ciudadano. La nueva ley proponía cambiar esta actitud. Reconoce la creciente importancia de la información en la sociedad e intenta impulsar una nueva mentalidad, en la cual la Administración se hace plenamente participativa en la nueva sociedad de la información, poniendo toda su información a disposición del público en lugar de simplemente mantenerla en sus archivos hasta la realización de una solicitud por parte del ciudadano.

La Ley fomenta como práctica normal la puesta de la información a disposición de la ciudadanía por medios electrónicos. La nueva actitud de poner la información a disposición del ciudadano antes de solicitarla recibe un nuevo impulso en el año 2002 con el E-Government Act.

Un informe del General Accounting Office en 2001 hizo constar que «mientras que es evidente que Internet trae nuevas oportunidades de mejorar el procedimiento de la provisión de servicios, la Administración debe ser consciente de las nuevas responsabilidades y retos que vienen conexos a estas oportunidades. Entre estos retos podemos señalar, entre otros, la necesidad de mantener un servicio enfocado al ciudadano, la protección de la intimidad personal, la implementación de protocolos efectivos para proteger la seguridad nacional, el mantenimiento correcto de los archivos electrónicos, el mantenimiento de una infraestructura efectiva y el aseguramiento de que la provisión de servicios electrónicos al ciudadano se realice de manera uniforme»[373].

La ley nació de la constatación de que la utilización de la informática, sobre todo de Internet, está llevando a una transformación rápida y fundamental de todo tipo de interacción social de las relaciones existentes entre ciudadanos, el sector privado y la Administración.

---

[373] Informe del General Accounting Office 01-959T, Electronic Government: Challenges must be Addressed with Effective Leadership and Management, 11 de julio de 2001.

La Ley tiene entre sus objetivos «promover el uso de Internet y de otras tecnologías de la información creando nuevas oportunidades para que los ciudadanos puedan participar activamente en las actividades del gobierno y promocionar la colaboración interadministrativa en la provisión de servicios electrónicos del gobierno» y contiene previsiones relativas a la disponibilidad de información en manos de la Administración en Internet, estándares para las páginas web de las Administraciones, la conservación de información en formato electrónico, el uso de la firma electrónica en los temas de contacto del ciudadano con la Administración, la protección de la intimidad, las medidas de seguridad aplicables a la información y el uso de datos de estadística.

1.3.3 Conclusiones

La Constitución norteamericana no establece un derecho explícito de acceso a la información administrativa. A pesar de la carencia de una regulación constitucional explícita, la legislación estadounidense ha ido construyendo un acervo normativo sobre el acceso a la información que obra en manos de los poderes públicos que, en su día, fue pionero, y que en muchos aspectos ha servido de base a normas similares introducidas en otros países.

En Estados Unidos, el acceso a la información administrativa ha evolucionado desde unos orígenes «corporativistas», durante los cuales la información se consideraba como un «patrimonio de la Administración» –cuya difusión solamente se realizaba según las condiciones fijadas por la propia Administración y era considerada como un instrumento de control político–, hasta la creación de una cultura en la cual el acceso a la información administrativa se considera como un elemento vital para facilitar la participación democrática de los ciudadanos.

Esta cultura de apertura ha sido impulsada por los Tribunales, que han apoyado la intención manifiesta del Congreso de fomentar el acceso del ciudadano a la información que se encuentre en manos de la Administración y han limitado de forma sucesiva las trabas que esta última pudiera interponer para su divulgación.

La legislación norteamericana más reciente ha debido adecuarse también al impacto de las nuevas tecnologías de la información, estableciendo que el derecho de acceso a la información administrativa alcanza también a la información que se encuentra almacenada en formatos electrónicos, y que la Administración debe, dentro de lo razonable, esforzarse en buscar la información dentro de sus bases de datos y entregarla en el formato solicitado por el peticionario.

Y es más, la legislación actual exige a la Administración un esfuerzo adicional: que considere, en todo momento, qué información es susceptible de divulgación y cómo pueda utilizar mejor las nuevas tecnologías de la información para ponerla a disposición de los ciudadanos, incluso sin que la soliciten.

Esta última legislación también ha efectuado cambios organizativos en las Agencias federales, creando estructuras y obligaciones nuevas en cuando a la forma de presentar la información y facilitando el acceso del ciudadano en el proceso de toma de decisiones de la Administración, fundamentándose en principios profundamente democráticos, convencidos de que la salud democrática del país solamente puede salir beneficiada si el ciudadano participa y controla la actividad de la Administración.

1.4 El impulso del Derecho Comunitario a la publicidad y transparencia de la Administración

Se ha criticado con frecuencia el déficit democrático de la Unión Europea. Es por ello que se ha impulsado, sobre la base del principio democrático, de forma muy notable en la Unión Europea, la publicidad y transparencia en la actuación de la Administración comunitaria.

Asimismo, el hecho de que Estados miembros como Suecia, Finlandia o Dinamarca tuviesen una larga tradición histórica en su derecho de reconocimiento como principios fundamentales de la transparencia y publicidad, además de un acceso generalizado a los archivos y registros administrativos, ha tenido también una influencia significativa en la potenciación de estos principios por la Unión Europea.

En el Tratado Constitutivo de la Comunidad Europea[374] ya existían algunas referencias a la transparencia[375], si bien el empuje se acelera a partir del Tratado de Ámsterdam, de tal forma que en el Tratado de la Unión Europea (TUE) de 7 de febrero de 1992, en el artículo primero, párrafo 2, se establece que las decisiones de la Unión serán tomadas no solo «de la forma más próxima a los ciudadanos», sino también «de la forma más abierta posible». Por otra parte, el acceso a los documentos de las instituciones de la Unión está también reconocido (artículo 255 TCEE). Finalmente, a nivel de Derecho primario, también se hace referencia a la transparencia en el artículo 1.2, con palabras prácticamente idénticas a las de los artículos 1.2 TUE y 11.3 del Tratado de Lisboa.

Sobre la base de estos dos últimos preceptos se elabora el Reglamento 1049/2001[376], que potencia a través del principio democrático una mayor participación de los ciudadanos en el proceso de toma de decisiones, para lo que el derecho a la información y el principio de transparencia juegan un papel esencial. También ese Reglamento acentúa en su considerando 2º que la transparencia consolida el principio democrático y el respeto de los derechos fundamentales. En este sentido, el artículo 1 del Reglamento 1049/2001 fija como objetivo el acceso más amplio posible a los documentos y que se facilite el ejercicio de este derecho, estableciéndose, sin embargo, un amplio abanico de excepciones a ese derecho en el artículo 4 que deben ser interpretadas restrictivamente, y así lo ha hecho la jurisprudencia.

En el seno del Consejo de Europa se han venido adoptando desde hace décadas iniciativas tanto en materia de acceso a la información pública como de protección de datos. En síntesis, la normativa sobre acceso a la

---

[374] Antiguos artículos 190 y ss. (hoy artículos 253 y ss)

[375] No solo en ese Tratado, sino en otros constitutivos como el TCECE, se hacía referencias a la transparencia: véase Cerrillo i Martínez. A. (1998). *La transparencia administrativa: Unión Europea y medio ambiente*. Valencia: Tirant lo Blanch, pp. 27 y ss.

[376] Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión DO L 145, de treintaiuno de mayo de 2001.

información pública es la determinante de la legalidad o no de la comunicación de información por parte de la Administración a los ciudadanos, también cuando incluya datos personales, salvo cuando se trata del propio afectado, en cuyo caso es de aplicación la normativa sobre protección de datos, que regula el denominado derecho de acceso.

Aunque será objeto de un posterior análisis con mayor profundidad, por el momento podemos advertir que, uno de los límites del derecho de acceso es "la intimidad y otros intereses legítimos privados", si bien no se trata de un límite absoluto, sino que cualquier restricción al derecho a acceder a la información debe ser necesaria y proporcionada. El posterior tratamiento de dichos datos se rige por la normativa sobre protección de datos.

En cuanto al Derecho de la Unión Europea, frente a la primera jurisprudencia del Tribunal de Luxemburgo, que habrá de ser cuanto menos, matizada, parece ir imponiéndose un acercamiento a la cuestión a partir de la normativa sobre acceso y, por tanto, en el que la ponderación es necesaria tan solo cuando el mismo puede menoscabar el derecho a la intimidad o a la integridad, en sentido amplio, no reducido a lo estrictamente personal o familiar, pero que no llega a cubrir, con carácter general, las actividades llevadas a cabo por cuenta o en relación con la Administración pública[377]. Además, comienza a abrirse paso la idea de que no toda información que contenga el nombre de una persona es, *per se*, información personal, sino que sólo tendrá esa consideración si por su objeto, finalidad o resultado, se trata de información que puede, influir en la autonomía personal del sujeto.

[377] Tiene singular interés, al respecto, el documento del Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. Background Paper Series, 1. En https://edps.europa.eu/sites/edp/files/publication/05-07_bp_accesstodocuments_en.pdf

1.5 La evolución en la relación de los derechos de protección de datos de carácter personal y de acceso a la información pública en el ámbito de la Unión Europea

La actual Directiva 95/46/CE[378] no establece los necesarios instrumentos para la conciliación entre el derecho de acceso a la información pública y el de protección de los datos de carácter personal presentes en la misma. Tan sólo encontramos una referencia en el Considerando 72[379]. Sin embargo, en el articulado de la norma, no se incluyó ninguna referencia ni, por tanto, ningún instrumento jurídico concreto que estableciera los parámetros regulatorios de dicha relación, de manera que simplemente se incluía un criterio interpretativo en relación con los principios a aplicar.

En el proceso evolutivo de regulación del derecho a la protección de datos es necesario hacer referencia también a dos hitos fundamentales, que van a su vez a afectar a las relaciones entre los dos derechos analizados. De una parte, la inclusión de la protección de datos como derecho fundamental en la Carta de Derechos Fundamentales de la Unión Europea[380], y de otra, la aprobación del Reglamento (CE) 45/2001[381]. Ésta, tampoco incluye en su articulado referencia alguna a las relaciones entre ambos derechos, si bien

---

[378] Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE L281 de 23.11.1995).

[379] Expresamente se afirme en el Considerando 72 Directiva 95/46/CE «considerando que la presente Directiva autoriza que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en la presente Directiva».

[380] Establece la Carta, en su artículo 8, que «1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas estará sujeto al control de una autoridad independiente».

[381] Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de doce de enero de 2001)

parece remitir este aspecto a la normativa de acceso a la información[382]. En el Considerando 15 encontramos una mención al artículo 255[383] del Tratado CE por el que se regulaba el derecho de acceso a la información de las instituciones comunitarias, y que fue la base del desarrollo del Reglamento 1049/2001. Es esta norma por la que se regirá la relación entre los derechos de acceso a la información y a la protección de datos de carácter personal en los documentos de las instituciones de la Unión Europea.

Hay que tener en cuenta, por tanto, que en el momento de aprobación de la Directiva 95/46/CE, el derecho de acceso se encontraba en pleno proceso de reconocimiento en la Unión Europea, de manera que ha sido fundamentalmente la jurisprudencia del Tribunal de Justicia de la Unión Europea la que ha establecido los parámetros de relación entre ambos derechos en el ámbito comunitario[384]. Gracias a la labor de los tribunales comunitarios se ha ido definiendo con mayor precisión y amplitud aquello que es accesible para el público en el ámbito de las Comunidades Europeas y de la Unión Europea, partiendo inicialmente de una definición muy acotada y restrictiva del mismo -puesto que solo se reconocía el acceso a escritos

---

[382] En su Considerando 15, la Directiva 95/46/CE establece que «el acceso a los documentos, incluidas las condiciones de acceso a los documentos que contengan datos personales, depende de las normas adoptadas sobre la base del artículo 255 del Tratado CE, cuyo ámbito de aplicación abarca los Títulos V y VI del Tratado de la Unión Europea».

[383] La nueva regulación de este derecho se encuentra en la actualidad en el artículo 15 del Tratado de Funcionamiento de la Unión Europea. Artículo 15 (antiguo artículo 255 TCE) 1. A fin de fomentar una buena gobernanza y de garantizar la participación de la sociedad civil, las instituciones, órganos y organismos de la Unión actuarán con el mayor respeto posible al principio de apertura. 2. Las sesiones del Parlamento Europeo serán públicas, así como las del Consejo en las que éste delibere y vote sobre un proyecto de acto legislativo. 3. Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte, con arreglo a los principios y las condiciones que se establecerán de conformidad con el presente apartado».

[384] Son especialmente relevantes, la Sentencia Tribunal de Justicia de la Unión Europea de 29 de junio de 2010, asunto C-28/08 P, Comisión contra Bavarian Lager, cuyo criterio ha sido completado por la Sentencia Tribunal de Justicia de la Unión Europea de 16 de julio de 2015, asunto C-615/13 P. Client Earth y PAN Europe contra EFSA, Comisión Europea y el Supervisor Europeo de Protección de Datos (SEPD)

que estuvieran contenidos en los archivos históricos, y solamente transcurridos treinta años desde su producción-, hasta su reconocimiento como derecho fundamental en la Carta de los Derechos Fundamentales de la Unión Europea, y su actual definición por el Reglamento 1049/2001, que reconoce un amplio derecho a los documentos de las instituciones[385], cuyo ámbito de aplicación está llamado a ampliarse a todas las instituciones de la Unión Europea, al regularse en el artículo 15 del Tratado de Funcionamiento de la Unión Europea.

Entre los límites que establece el Reglamento 1049/2001 está la protección de los datos de carácter personal a los que alude en su Considerando 11[386] y en el artículo 4.1 b)[387]. Estas dos referencias han sido interpretadas por la jurisprudencia comunitaria, especialmente destacamos la Sentencia Tribunal de Justicia de la Unión Europea de 29 de junio de 2010, asunto C-28/08 P, Comisión contra Bavarian Lager, en el sentido de constituir un claro vínculo de reenvío entre los Reglamentos 1049/2001 y 45/2001, de manera que la jurisprudencia comunitaria ha interpretado aquel artículo como un reenvío a la normativa de protección de datos. Por tanto, el Reglamento 45/2001 se considera plenamente aplicable cuando se insta una solicitud de

---

[385] Debemos destacar las afirmaciones del Abogado General Philippe Leger, presentadas en fecha 10 de julio 2001 en relación a la Sentencia del Tribunal de Justicia de las Comunidades Europeas de 6 de diciembre de 2001, asunto C-353/99 P, Consejo c. Hautala. En el Considerando 79 de sus Conclusiones, el Abogado General declara que «la calificación del derecho de acceso a documentos como derecho fundamental constituye una nueva etapa en la labor de reconocimiento y jerarquización de dicho principio dentro del ordenamiento jurídico comunitario.

[386] Establece este considerando que: «En principio, todos los documentos de las instituciones deben ser accesibles al público. No obstante, deben ser protegidos determinados intereses públicos y privados a través de excepciones. Conviene que, cuando sea necesario, las instituciones puedan proteger sus consultas y deliberaciones internas con el fin de salvaguardar su capacidad para ejercer sus funciones. Al evaluar las excepciones, las instituciones deben tener en cuenta los principios vigentes en la legislación comunitaria relativos a la protección de los datos personales, en todos los ámbitos de actividad de la Unión».

[387] El artículo 4 declara: «1. Las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de: […] b) la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales…».

acceso que contiene datos de carácter personal[388]. Esta Sentencia establece explícitamente la relación entre ambos Reglamentos, y la aplicabilidad de la normativa de protección de datos cuando se alude a la excepción contemplada en el artículo 4.1.b) del Reglamento 1049/2001.

Pues bien, en este sentido, este Reglamento 45/2001 exige, en su artículo 8, para la comunicación o transmisión de datos de carácter personal a terceros sin consentimiento expreso de los afectados que:

> *«a) el destinatario demuestre que los datos son necesarios para el cumplimiento de una misión de interés público o son inherentes al ejercicio del poder público, o b) el destinatario demuestre la necesidad de que se le transmitan los datos y no existan motivos para suponer que ello pudiera perjudicar los intereses legítimos del interesado».*

Por tanto, hasta la actualidad[389], el hecho de que por aplicación del artículo 4.1.b) del Reglamento 1049/2001 en las solicitudes de acceso sea de aplicación directamente lo prescrito por la normativa de protección de datos, determina la exigencia de que medie consentimiento o que el destinatario demuestre la necesidad de que se le transmitan los datos y que no existen motivos para suponer que ello pudiera perjudicar los intereses legítimos del interesado, constituyendo además dos condiciones cumulativas[390], de

---

[388] Esta interpretación jurisprudencial ha llevado a un inevitable cambio de postura de las instituciones comunitarias, y muy particularmente del Supervisor Europeo de Protección de Datos, que en 2005 había publicado un documento sobre directrices en relación con el «Acceso del público a los documentos y protección de datos», que se ha visto obligado a modificar tras la resolución del asunto Bavarian Lager, en su documento de 2011 «Public Access to documents containing personal data after the Bavarian Lager ruling». Podemos acceder al texto de este documento en el link https://edps.europa.eu/sites/edp/files/publication/11-03-24_bavarian_lager_en.pdf

[389] A la luz de lo dispuesto por el Reglamento, esta interpretación es susceptible de variar, en aplicación de los principios explicitados en el Considerando 154 y en su artículo 86.

[390] Apartados 45 y 46 de la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2015, ClientEarth/PAN Europe contra EFSA y Comisión, asunto C-615/13 P «45 A tenor del artículo 8, letra b), del Reglamento nº 45/2001, los datos personales sólo se transmitirán en principio si el destinatario demuestra la necesidad de que se le transmitan los datos y no existen motivos para suponer que ello pudiera perjudicar los intereses legítimos del interesado»; y «46 De los propios

manera que «en ese contexto corresponde en primer lugar a quien solicita esa transmisión demostrar su necesidad. Si aporta esa prueba, incumbe entonces a la institución interesada verificar si no hay ningún motivo para suponer que esa transmisión podría perjudicar los intereses legítimos de la persona interesada. En defecto de un motivo de esa clase, debe accederse a la transmisión solicitada, mientras que en caso contrario la institución interesada ha de ponderar los diferentes intereses contrapuestos para pronunciarse sobre la solicitud de acceso»[391].

Es necesario, por tanto, en la interpretación actual de la cuestión, que se esgriman razones que justifiquen la necesidad de la transmisión de la información, para que pueda procederse a la ponderación entre derechos, esto es, sin que con la mera demostración de la necesidad prime el de acceso a la información, y todo ello a pesar de que, en principio, el solicitante no tenga por qué motivar su solicitud, según lo dispuesto por el artículo 6[392] del Reglamento 1049/2001.

En la Sentencia ClientEarth/PAN Europe, el TJUE justifica esta postura aludiendo que no cabe atribuir en general una preeminencia automática al objetivo de transparencia frente al derecho a la protección de los datos de carácter personal[393], si bien en el caso concreto no solo reconoce la

términos de esa disposición resulta, como el Tribunal General juzgó válidamente en el apartado 83 de la sentencia recurrida, que somete la transmisión de datos personales a la concurrencia de dos condiciones acumulativas».

391 Apartado 47 de la Sentencia del Tribunal de Justicia de la Unión Europea, de 16 de julio de 2015, ClientEarth/PAN Europe contra EFSA y Comisión, asunto C-615/13 P (véanse, en ese sentido, las sentencias Comisión/Bavarian Lager, C-28/08 P, EU:C:2010:378, § 77 y § 78, y Strack/Comisión, C-127/13 P, EU:C:2014:2250, § 107 y § 108; véase también, en el mismo sentido, la sentencia Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, § 85).

392 Artículo 6 Solicitudes «1. Las solicitudes de acceso a un documento deberán formularse en cualquier forma escrita, incluido el formato electrónico, en una de las lenguas a que se refiere el artículo 314 del Tratado CE y de manera lo suficientemente precisa para permitir que la institución identifique el documento de que se trate. El solicitante no estará obligado a justificar su solicitud».

393 El apartado 51 establece: «No obstante, el Tribunal de Justicia ha juzgado en ese sentido que no cabe atribuir en general una preeminencia automática al objetivo de transparencia frente al derecho a la protección de los datos de carácter personal (sentencia Volker und Markus Schecke y Eifert, C-92/09 y C-93/09, EU:C:2010:662, § 85)».

existencia de esa necesidad, sino que en la apreciación de si la divulgación solicitada puede perjudicar concreta y efectivamente el interés protegido, concluye que no ha quedado demostrada, por lo que procede a anular la decisión que denegaba el acceso en primer lugar[394].

De todo lo anterior se deduce que, hasta la actualidad, las normas comunitarias de protección de datos han optado por no regular la relación entre el ejercicio de este derecho y el de acceso a la información y, si bien en el ámbito netamente comunitario, desde el año 2001, en aplicación del considerando 15 del Reglamento 45/2001, las reglas que regulan el acceso a los documentos en los que figuran datos de carácter personal se rigen por las normas de acceso a la información, la interpretación ha sido el reenvío directo a las normas reguladoras del derecho a la protección de los datos de carácter personal y a todos los principios que son de aplicación al mismo. De manera que, aunque no puede excluirse de manera absoluta el acceso a la información por causa de la protección de los datos, se debe velar en todo caso por que se cumplan los requisitos para la comunicación o transmisión de los datos previstos por los artículos 7, 8 y 9 del Reglamento 45/2001.

En definitiva, un constante reenvío entre normas que no ha alcanzado a establecer claramente los parámetros de relación entre dos derechos que en el entorno comunitario tienen la consideración de fundamentales y que deben ser por tanto respetados de manera equilibrada sin que exista preeminencia automática de uno sobre otro, pese a que las instituciones comunitarias, por lo general, han sido más proclives a la defensa de los datos de carácter personal que al reconocimiento del derecho de acceso a los documentos que los contiene.

---

[394] Puesto que se alinea en este sentido con la ya arraigada doctrina jurisprudencial del TJUE que considera que las excepciones al derecho de acceso no solo deben ser interpretadas restrictivamente, sino que además debe comprobarse, en cada caso concreto, la existencia de riesgo de un perjuicio concreto y efectivo para el interés público.

1.6 Los esperables efectos de la nueva regulación en el ámbito comunitario

Dado que, conforme a los estipulados del artículo 2.3 del RGPD[395], el Reglamento 45/2001 sigue siendo de aplicación al tratamiento de datos de carácter personal por parte de las instituciones, órganos y organismos de la Unión, y que éste «y otros actos jurídicos de la Unión aplicables a dicho tratamiento de datos de carácter personal se adaptarán a los principios y normas del presente Reglamento de conformidad con su artículo 98[396]», tenemos que entender que también se aplicará en este ámbito, el principio de accesibilidad a los documentos oficiales con datos de carácter personal, según se establece en el artículo 86 del RGPD.

Esto es, debe entenderse que también será necesaria una nueva lectura del Reglamento 45/2001, en relación a su aplicación por reenvío de la excepción prevista en el artículo 4.1. b)[397] del Reglamento 1049/2001. Por ello, habrá de hacerse una nueva interpretación del artículo 8 del Reglamento 45/2001, por cuando el Reglamento presupone el interés público de las solicitudes de acceso a la información oficial.

Como ya hemos indicado, esto no quiere decir que todos los documentos que tengan datos de carácter personal, fuera de los excluidos de tratamiento por el artículo 9.1. del Reglamento, vayan a ser directamente accesibles, sino que en los criterios reiterados por la jurisprudencia de demostración de

---

[395] Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) [DOUE L 119, 4.5.2016]

[396] Artículo 98 «La Comisión presentará, si procede, propuestas legislativas para modificar otros actos jurídicos de la Unión en materia de protección de datos personales, a fin de garantizar la protección uniforme y coherente de las personas físicas en relación con el tratamiento. Se tratará en particular de las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento por parte de las instituciones, órganos, y organismos de la Unión y a la libre circulación de tales datos».

[397] Artículo 4 «1. Las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de […] b) la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales».

la necesidad de acceder a los datos y de la legitimidad de la misma, a través de la preceptiva ponderación de intereses, se puede introducir un mayor equilibrio entre las partes.

De esta manera, el encargado del tratamiento, deberá llevar a cabo la aplicación de la excepción del artículo 4.1.b) del Reglamento 1049/2001, interpretando lo establecido por el artículo 8 del Reglamento 45/2001, a la luz de los principios de licitud del tratamiento explicitados por el artículo 6 del RGPD, en sus apartados 1 y 4.

En definitiva, seguirá siendo necesaria la ponderación de intereses, pero puede presuponerse la existencia del requisito de demostración de la necesidad de la comunicación en interés público que el Reglamento adjudica a todas las solicitudes de acceso referidas a documentos oficiales en posesión de las autoridades públicas[398] que contengas datos de carácter personal.

Habrá que esperar, no obstante, a la entrada en vigor del RGPD y a su ulterior interpretación por los Tribunales de Justicia para verificar si la calificación de interés público de la solicitud de acceso es suficiente en aras de la acreditación de la necesidad de conocer los datos, más en línea con la expresa declaración del artículo 6 del Reglamento 1049/2001, que no exige motivación de la solicitud de acceso, si bien no parece un paso muy fácil de conseguir de las autoridades comunitarias, hasta ahora tan proclives hacia la protección de los datos frente al derecho de acceso, todo ello pese a reconocerse en todos los niveles normativos de la Unión el carácter fundamental de ambos derechos.

[398] Interpretadas éstas en el sentido más amplio posible que lleva a cabo el Considerando 154 RGPD «La referencia a autoridades y organismos públicos debe incluir, en este contexto, a todas las autoridades u otros organismos a los que se aplica el Derecho de los Estados miembros sobre el acceso del público a documentos».

1.7 Desarrollo del principio de transparencia a través de la jurisprudencia del Tribunal de Justicia

El punto de mayor conflictividad del Reglamento 1049/2001 se encuentra en las amplias y, en algún caso, poco concretas excepciones al derecho de acceso de los ciudadanos a los documentos, por lo que el Tribunal de Justicia de las Comunidades Europeas (TJCE) se ha enfrentado a diversos litigios sobre el tema, apoyándose en su argumentación de manera primordial en el significado del principio democrático y la transparencia.

En este sentido, el Tribunal de Primera Instancia de las Comunidades Europeas, en su Sentencia de 8 de noviembre de 2007, asunto Bavarian Lager contra Comisión[399], considera que las excepciones del artículo 4 del Reglamento 1049/2001 deben interpretarse y aplicarse restrictivamente para que no se frustre la aplicación del principio general de acceso a los documentos (apartados 93 y94), y asimismo determina que el Reglamento 1049/2001 tienen como objetivo la garantía del máximo de transparencia y el promover buenas prácticas administrativas (artículo 98). En base a estos presupuestos, el Tribunal de Primera Instancia hace una interpretación restrictiva de la excepción al derecho de acceso frente a la protección de la intimidad e integridad de la persona[400] [artículo 4.1.b) del Reglamento], estableciendo que, aunque el concepto de vida privada sea amplio, eso no significa que todos los datos personales haya que incluirlos necesariamente en el concepto de intimidad (§ 118), por lo que la aplicación de esa excepción debe realizarse de forma concreta y constar en la motivación de la decisión (§ 151), lo cual no se produce en el caso concreto.

---

[399] Sentencia Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager contra Comisión, Asunto T-194/04.

[400] Guichot Reina, E. (2008). Un paso decisivo en la clasificación de las relaciones entre derecho de acceso y derecho a la protección de datos: la Sentencia del TPI de 8 de noviembre de 2007, Bavarian Lage/Comisión, t-194/04. *Revista Española de Derecho Europeo, 27*. Madrid: Civitas. pp. 329 y ss., esp. pp. 343 y ss.

El Tribunal de Justicia (Gran Sala) en la Sentencia de 1 de julio de 2008, asunto Maurizio Turco contra Consejo de la Unión Europea[401], vincula, en primer lugar, de manera nítida, con efectos recíprocos, el principio democrático y la transparencia cuando establece «que el principio de transparencia refuerza la democracia al permitir que los ciudadanos controlen toda la información que ha constituido el fundamento de un acto legislativo» (§ 46). Por otra parte, en segundo lugar, dice el Tribunal en su apartado 59 que la transparencia permite que las divergencias se debatan ampliamente, lo que confiere una mayor legitimidad a las instituciones a los ojos de los ciudadanos europeos y a aumentar su confianza en éstas[402]. Y sigue argumentando el Tribunal que precisamente «la falta de información y de debate puede suscitar dudas en los ciudadanos no solo en cuanto a la legalidad de un acto aislado, sino también en cuanto a la legitimidad del proceso de toma de decisiones en su totalidad».

Finalmente, vuelve el Tribunal de Luxemburgo a vincular principio democrático y transparencia como medio de hacer efectiva la participación del ciudadano y legitimación de la Administración, y considera que en la ponderación entre el mantenimiento de la confidencialidad del dictamen del servicio jurídico de la Comisión y el interés público superior que pueda suponer la divulgación (artículo 1.2 del Reglamento 1049/2001), en este caso concreto las cuestiones jurídicas surgidas en el debate sobre las iniciativas legislativas «puede aumentar la transparencia y la apertura del proceso legislativo, y puede reforzar el derecho democrático de los ciudadanos europeos a controlar la información que constituyó la base de un acto legislativo» (§ 67).

La tendencia mantenida por el Tribunal de Justicia de reforzamiento de un derecho de acceso muy amplio a los documentos de las instituciones y de restricción de las excepciones es una constante mantenida en su

---

401 Sentencia Tribunal de Justica (Gran Sala) de 1 de julio de 2008, Reino de Suecia y Maurizio Turco contra Consejo de la Unión Europea, asuntos acumulados C- 39/05 P y C-52/05 P.

402 «El conocimiento de la actuación de la Administración, y en su caso la participación del ciudadano, legitima su tarea, y desde luego la facilita, lo que podrá hacerla más eficiente».

jurisprudencia, para lo cual se basa en el principio democrático, la publicidad y la transparencia. En este sentido, la Sentencia del Tribunal de Justicia[403], establece una interpretación restrictiva del artículo 4.5 del Reglamento 1049/2001[404] cuando dice que ese precepto no dota a un Estado miembro «de un derecho de veto general e incondicional para oponerse discrecionalmente a la divulgación de documentos procedentes de él y en poder de una institución de la Unión Europea» (§ 75)[405]. En este sentido, esa sentencia entiende que el artículo 4.5 del Reglamento no puede ser interpretado aisladamente, sino que debe hacerse en el contexto del proceso de adopción de la decisión comunitaria, y debe entablarse un diálogo leal sobre la posible aplicación de las excepciones al acceso establecidas en el artículo 4, apartados 1 a 3, del Reglamento (§ 86), y en cualquier caso, el Estado miembro debe motivar su oposición a la divulgación del documentos sobre la base de esas excepciones (§ 87).

Finamente, debe ponerse de relieve la doctrina mantenida por el Tribunal en esa sentencia cuando dice que el derecho de acceso del público a los documentos de las instituciones, garantizado en el artículo 1 del Reglamento 1049/2001, está ligado al carácter democrático de éstas, y que ese Reglamento tiene por objeto garantizar el acceso más amplio posible a los documentos, y las excepciones a este derecho deben interpretarse y aplicarse en sentido estricto (§ 66).

---

[403] Sentencia Tribunal de Justica (Gran Sala) de 18 de diciembre de 2007, Reino de Suecia y Maurizio Turco contra Consejo de la Unión Europea, asunto C- 64/05 P.

[404] Este precepto, tal como está redactado, concede amplias posibilidades a los Estados miembros para vetar el acceso de los ciudadanos a los documentos; sin embargo, la jurisprudencia del Tribunal de Justicia ha restringido ese derecho de veto con la introducción de determinadas condiciones restrictivas de su ambigüedad.

[405] Esta misma doctrina restrictiva de la interpretación del artículo 4.5 del Reglamento es mantenida en otra jurisprudencia del Tribunal de Justicia; así, entre otras, en las Sentencias del Tribunal de Primera Instancia (Sala Segunda) de 19 de enero de 2010, Co-Frutta Soc. coop. Contra Comisión Europea, asuntos acumulados T-355/04 y T-446/04, en su § 80, o bien en la Sentencia del Tribunal de Justicia (Gran Sala) de 26 de enero de 2010, Internationaler Hilfsfonds contra Comisión Europea, asunto C-362/08 P, en su § 56.

1.8 Incidencia del Reglamento en las relaciones entre el derecho de acceso a la información y el derecho a la protección de datos de carácter personal en el ámbito interno español

Hasta la aprobación de la LTBG, no había referencia alguna a las relaciones existentes entre ambos derechos, dado que la LOPD no recoge referencia alguna al derecho de acceso a la información, únicamente contemplada desde la estricta perspectiva de la comunicación de datos prevista por los artículos 6 y 11 LOPD, y la normativa básica de acceso a la información, regulada en el artículo 37[406] de la Ley 30/1992 LRJPAC, establecía un estricto régimen de legitimación cuando los documentos contuvieran «datos nominativos» o que pudieran afectar a la intimidad de las personas.

La tensión existente entra ambos derechos se dilucidaba, tanto en sede administrativa como jurisprudencial, en una clara preeminencia del derecho a la protección de datos sobre el derecho de acceso a la información, alimentada por el ineludible hecho de que mientras que el derecho a la protección de datos ha sido reconocido como un derecho fundamental, de carácter autónomo, sobre la base del artículo 18.4[407] de la CE, el acceso a la información sigue siendo considerado por el legislador como un derecho

[406] La Disposición derogatoria única de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE núm. 236, de 2 de octubre de 2015, declara expresamente en su apartado 2 que «quedan derogadas expresamente las siguientes disposiciones: a) Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común». La regulación de acceso a la información se regirá por el artículo 13 de dicha norma, relativo a los derechos de las personas en sus relaciones con las Administraciones Públicas. Así, «quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos: […] d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico».

[407] Artículo 18.4 CE «La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos».

subjetivo ordinario, que no goza por tanto de la protección que se otorga por la Constitución a los derechos fundamentales[408].

La diferente cualificación de ambos derechos hace que su conciliación se vuelva harto complicada, si bien la LTBG ha venido a establecer un nuevo sistema de relación entre ambos derechos, que supone la necesidad de su ponderación para determinar en cada caso concreto si debe darse acceso a la información o si por el contrario debe denegarse, por primar la protección de datos de carácter personal.

Y esto porque, a pesar de que a la luz de la LOPD el acceso a la información debe ser considerado como una cesión de datos, por lo que en principio le es aplicable lo dispuesto en los artículos 6 y 11 de dicha norma[409], la LTBG ha sido el título habilitante que conecta con el artículo 11 LOPD y que determina, a través de su artículo 15, que será la LTBG la norma aplicable a la hora de dilucidar si se debe dar acceso a la información pública en manos de los sujetos obligados por la misma o, si por el contrario, se debe denegar el mismo en aras de la protección de datos de carácter personal.

Es pues, el órgano o entidad que posee la información quien debe decidir, a través del procedimiento de acceso a la información previsto en los artículos

---

[408] La doctrina critica el hecho de que pese a que no solo a nivel comunitario, sino también a nivel internacional, y notablemente, en el marco del Consejo de Europa de los Derechos Humanos, el acceso a la información se considera un derecho fundamental, mientras que nuestro legislador nacional ha regulado el derecho vinculándolo únicamente al artículo 105 b) CE «La ley regulará: […] b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas» y regulándolo como un derecho ordinario.

[409] Como recuerda Piñar Mañas, antes de la aprobación de la aprobación de la LTBG, la Agencia de Protección de Datos emitió un Informe de 5 de junio de 2012, en el que «llama la atención acerca de la necesidad de que la transparencia sea «congruente con los principios que conforman el derecho fundamental a la protección de datos de carácter personal». Señala que la divulgación de la información que obre en poder de los sujetos obligados implicará, como punto de partida, la realización de un tratamiento específico sobre los datos de carácter personal que tal información pudiera contener … de manera que solo cabrá conceder el acceso si el mismo es conforme no solo con la Ley de Transparencia sino asimismo con la LOPD». Piñar Mañas, J. L. (2014). Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. En Piñar Mañas, J.L. (Coord.). *Transparencia, acceso a la información y protección de datos.* Madrid: Reus.

17 y siguientes LTBG, a través de la preceptiva ponderación entre ambos derechos, si se concede el acceso o bien se deniega, aplicando o dispuesto en el artículo 15, y teniendo para ello en cuenta los criterios interpretativos aprobados por el Consejo de Transparencia y buen Gobierno en conjunción con la Agencia de Protección de Datos, según lo dispuesto en la Disposición Adicional quinta[410] de la Ley 19/2013, de 9 de diciembre[411].

Del artículo 15 y de los criterios interpretativos se deduce, de un lado, la voluntad de primar el acceso a la información sobre la protección de datos cuando se trata de datos meramente identificativos, previstos por el artículo 15.2 LTBG, y por otro lado, que mientras que los límites al acceso previstos por el artículo 14 LTBG «podrán ser de aplicación», cuando se trata de datos de carácter personal esta excepción opera de manera automática, notablemente cuando se trata de datos especialmente protegidos, para los cuales el artículo 15, en su apartado 1 dispone que es necesario el consentimiento expreso del interesado[412].

Par el resto de los datos, y salvo que sea posible la disociación de los mismos, en cuyo caso la accesibilidad prima sobre la protección de los datos (artículo 15.4), el apartado 3 de este artículo 15 LTBG establece unos criterios de ponderación para decidir qué debe primar en cada caso

---

[410] Disposición adicional quinta. LTBG Colaboración con la Agencia Española de Protección de Datos. «El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre».

[411] Informe de 23 de marzo de 2015, sobre acceso a datos de las retribuciones de funcionarios y el Criterio interpretativo 2/2015, de 24 de junio de 2015, sobre la aplicación de los límites al derecho de acceso a la información. Ambos documentos pueden consultarse en http://www.consejodetransparencia.es/ct_Home/consejo/criterios_informes_consultas_documentacion

[412] Salvo cuando hayan sido hechos manifiestamente públicos por el interesado, en el caso del párrafo 1, o si el acceso estuviera amparado por una norma con rango de Ley, para los datos recogidos en el párrafo 2.

concreto[413]. Esto es, los criterios de ponderación entre ambos derechos son los establecidos por el artículo 15 de la LTBG, sin perjuicio de que para su aplicación sea necesario acudir a las definiciones de datos de carácter personal previstas por la LOPD.

La aprobación del RGPD está llamada a la producción de importantes cambios en la LOPD, al menos en las materias afectadas por el Derecho de la Unión Europea. Y, sin duda, este cambio normativo vendrá a afectar al acceso a la información pública que contenga datos personales, en la actualidad regulada por el artículo 15 LTBG.

Sin embargo, en nuestro ordenamiento nacional, los parámetros de relación entre ambos derechos son sustancialmente divergentes del caso europeo, no solo debido a que en España la reticencia a considerar el derecho de acceso como derecho fundamental pone en la difícil tesitura de ponderar dos derechos cuyo reconocimiento y protección son sustancialmente diferentes, sino también por el hecho de que el legislador sí ha tomado la decisión de

---

[413] Artículo 15. *Protección de datos personales.* «[…] 3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal. Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios: a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos. c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos. d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad». Ha sido bastante criticado por la doctrina que, frente al normal criterio del transcurso de un tiempo aproximado de 20 años, la norma haya recogido las limitaciones que viniera a establecer para el acceso a los documentos la Ley de Patrimonio Histórico Español, cuyos criterios de 25 o 50 años no solo parecen excesivos, sino que se obligan «a transitar a diario el territorio de la incertidumbre cuando se presume una longevidad del ciudadano bastante superada por la esperanza de vida actual» Martínez Martínez, R. (2014). De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.) *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Thomson-Reuters Aranzadi, p. 244.

incluir los parámetros de la conciliación entre ambos derechos en una única norma jurídica, la LTBG, sin que se produzcan reenvíos[414].

En este sentido, no es descartable pensar en la posible necesidad de modificación de estos criterios, una vez que se produzca la modificación de la normativa de protección de datos de carácter personal, para adecuarla a lo previsto por el Reglamento, sobre todo en el sentido de incluir el carácter de interés legítimo de la consulta de documentos y en cuanto a la incorporación de los criterios de finalidad del tratamiento, sobre todo por lo que se refiere a la licitud proporcionalidad de los mismos, previstos por el artículo 6 del RGPD, lo que constituiría un criterio mucho más adecuado al meramente temporal que parece acoger en la actualidad nuestro ordenamiento jurídico, en defecto de consentimiento del afectado, para la ponderación de los derechos en juego, según se establece en el artículo 15.3. a) LTBG.

[414] Sin perjuicio de que se deba acudir a los criterios establecidos en la normativa de protección de datos para el ulterior tratamiento de los mismos, una vez que se ha obtenido el acceso por la vía de la LTBG, según lo dispuesto por su artículo 15.5.

2 EL DERECHO A LA INFORMACIÓN, LA PUBLICIDAD Y TRANSPARENCIA EN LAS RELACIONES ENTRE LA ADMINISTRACIÓN, EL CIUDADANO Y EL PÚBLICO

2.1 Introducción

Es una opinión generalizada entre la ciudadanía la necesidad de que la transparencia se proyecte sobre todos los ámbitos de la actividad pública. Es más, se exige que no solo deba conocerse la actuación resultante del ejercicio del poder público, sino también todo lo relacionado con la toma de decisiones, sus motivos y sus consecuencias.

Si con carácter general ese deber de transparencia ha aparecido difuminado en los textos constitucionales y legales –cuando lo ha hecho, y dependiendo de cada coyuntura social y política– en tiempos más recientes se está revitalizando su exigibilidad, tanto en ámbitos nacionales, como supranacionales.

De tal modo, frente al estado de cosas resultante de la tradicional marginación de la ciudadanía por el poder, hoy en día se tiende a posibilitar, aunque en diversa medida, el conocimiento por la sociedad del modo es que se desarrolla la gestión pública, con la suficiente justificación de los actos adoptados en dicha función.

La expectativa de transparencia puede tener como fin atajar la corrupción, así como conseguir una mayor eficiencia y eficacia de la utilización de los recursos públicos, y también una mayor legitimidad de las instituciones públicas. En todo caso, indudablemente con ella se abre una vía para limitar y condicionar la discrecionalidad del poder público, al tiempo que permite exigir la responsabilidad por su gestión.

2.2 Derecho a la información y cuentas públicas

2.2.1 El control de las cuentas públicas y la transparencia

Si bien el control de las cuentas públicas puede ser llevado a cabo a través de diversos mecanismos y procedimientos, para asegurar su conocimiento social es necesario instituir políticas de transparencia, es decir, actuaciones que posibiliten la apertura y disponibilidad de la información sobre su resultado.

Como hemos señalado antes, unos y otros conforman diversos aspectos de la rendición de cuentas, mientras que ésta en su relación con la transparencia no ha venido funcionando en nuestro país. No en balde, en la legislación española, desde una perspectiva formal, la rendición de cuentas consiste en la remisión de las mismas a los órganos fiscalizadores para su censura, es decir, su examen y aprobación y, en su caso, exigencia de responsabilidades[415].

En lo que nos ocupa, lo que debe determinarse es si esos órganos operan con transparencia respecto a la función que han realizado y la información que les ha suministrado, ya que las instituciones de control encargadas de la fiscalización de la actividad administrativa son una fuente directa de información.

Puede considerarse al respecto que el trabajo de los órganos de control externo alcanza su máximo sentido con la publicidad del mismo, con la comunicación a la sociedad de dicho análisis, pues lo contrario debilita la eficacia de su labor[416]. Frente a ello, nuestro país responde en este aspecto

---

[415] Así, Pascual García, J. (2014). *Régimen jurídico del gasto público. Presupuestación, ejecución y control*, Madrid: Boletín Oficial del Estado, p. 645.

[416] Véase Erbiti Zabalza, F. (2003). La comunicación: asignatura pendiente de las instituciones de control. *Auditoría Pública, 30*, pp. 4-5, para quien sería paradójico que una institución de control que predica la transparencia en la gestión de los fondos públicos como uno de los principios fundamentales, no la practicara en su propio trabajo. En este sentido, entiende Álvarez Martín, J. A. (2012). *El control de los recursos públicos condición inevitable de la democracia real*. Málaga: Fundación Asesores Legales, pp 76-77, que limitar la información y su difusión no favorece a los

a los caracteres de los sistemas de control de tipo jurisdiccional, en los que la publicidad que se realiza de esa información a la sociedad está muy desvirtuada, frente al sistema anglosajón, donde está más asentada y los órganos de control se han convertido en fuente informativa y su trabajo interesa cada vez más a la opinión pública[417].

En nuestro caso, si por un lado no se establece ninguna obligación de publicidad de los informes y resultados de las actuaciones de control interno, por el otro, en cuanto a los órganos de control externo, el artículo 136 CE solo dispone que el Tribunal de Cuentas remitirá a las Cortes Generales un informe anual en el que, cuando proceda, comunicará las infracciones o responsabilidades en que, a su juicio, se hubiere incurrido, memoria que debe ser publicada en el Boletín Oficial del Estado, al igual que los demás informes resultantes de su fiscalización.

No obstante, se viene entendiendo que sigue habiendo ausencias importantes tanto en materia de rendición de cuentas como de auditoría pública, así como que hay una notable falta de transparencia respecto a sus actuaciones sobre determinados extremos, o, siendo pública esa información (infracciones detectadas, responsabilidades declaradas, etc.), no se ofrece de una forma sistemática o fácilmente accesible, o no permite conocer de una forma detallada y completa todos los extremos que sería de interés.

Una de las carencias que en este ámbito se viene señalando es lo que estos órganos tardan en dar la información y la manera en la que la ofrecen, poco accesible para el ciudadano medio e incompleta. Por su complejidad y contenido tecnificado, distan de ser un instrumento adecuado de

---

órganos de control, y de hecho la difusión del resultado de la fiscalización ha conseguido atraer la atención de una sociedad cada vez más preocupada por el destino y la gestión de los fondos públicos.

[417] Véase Álvarez Martín, J. A. (2012), *op. cit*., pp. 75 y 102-103, quien señala que, en los EEUU, la Governmet Accountability Office (GAO) da publicidad de sus informes y testimonio en internet, actualizándolos diariamente, abarcando todas sus tareas y objetivos, sean internos o de control externo, mientras que en Gran Bretaña corre a cargo del Controller Auditor General (C&AG) junto con la National Audit Office (NAO)

conocimiento, a lo que también contribuye su gran volumen, que es lo que se ha dado en llamar desinformación técnica y desinformación por exceso[418].

2.2.2 La transparencia y el uso y destino de los recursos económicos

2.2.2.1 Ciudadanía y conocimiento de los asuntos públicos

La transparencia sobre los aspectos o elementos económicos de las decisiones públicas es todavía más exigible si cabe en momentos de crisis económica, en los que la ciudadanía quiere saber qué uso se hace de los recursos públicos. No en balde, uno de los rasgos de la sociedad contemporánea es su interés por conocer las decisiones que le afectan, es decir, cómo y por qué se han adoptado.

De ahí la necesidad de que se establezcan los mecanismos adecuados para permitir que los ciudadanos puedan informarse, para que les sea fácil e inmediato conocer todas las fases y circunstancias que han llevado a la decisión adoptada y sus consecuencias. Es evidente que lo anterior se encuentra en la esencia misma de la transparencia, como conjunto de principios y obligaciones que determinan una forma de actuar de la Administración, que debe posibilitarse a través de diversas vías.

Las situaciones y sucesos que cotidianamente se van conociendo a través de los medios de comunicación social, generan una creciente desconfianza de los ciudadanos en las autoridades y funcionarios, pero también en las instituciones. Ésta se ve incrementada por la opacidad tradicional de las cuestiones públicas en nuestro país, es decir, por la falta de información sobre la gestión de los asuntos públicos y, en este caso, sobre cómo y dónde

---

[418] Harden, I. (2001). Citizenship and Information. *European Public Law*, *vol. 7, Issue 2*. Países Bajos: Kluwer Law International, p. 175, para quien la información que debe ser pública, para que sea útil, *debe* ser cuidadosamente seleccionada, organizada *e interpretada. En* este sentido, señala igualmente Heald, D. (2006). Varieties of Transparency. En Hood, C. y Heald, D. (Eds.). *Transparency. The Key to Better Governance?,* Oxford: Oxford University Press, pp. 42-45, que entre los obstáculos a la transparencia del gasto público se encuentran las dificultades con respecto al volumen y la complejidad de la información, que impiden una transparencia efectiva, que se puede atribuir en parte al material técnico complejo y la comprensión pública limitada de las estructuras institucionales, o el no suministro de información en rendición de cuentas.

se gastan los recursos públicos, a los que todos contribuimos, quién ha decidido su destino y las razones para hacerlo.

Realmente, la sola disponibilidad de la información muchas veces no es suficiente, pues debe concurrir la capacidad para analizarla y usarla eficazmente, lo que remite a la forma de hacer públicos los datos, y de ahí que en el núcleo de la transparencia se encuentre también la exigencia de que la realidad que subyace en el gasto público sea visible y comprensible para sus destinatarios[419].

En lo que atañe al conocimiento de las cuentas públicas, su exigencia encuentra también su razón de ser en los ejes sobre los que se sustenta la transparencia, sus dos finalidades principales, el conocimiento de las mismas y su control. Asimismo, hay que considerar su carácter preventivo de conductas o prácticas indeseadas.

2.2.2.2 La rendición de cuentas

En los sistemas anglosajones el concepto de transparencia está estrechamente relacionado con aquellos que suponen un control del ejercicio del poder público.

El término que se viene utilizando en ellos, también adoptado por organismos internacionales como la OCDE, es el de accountability, que carece de equivalente preciso en castellano, siendo el más común el de «rendición de cuentas». Si bien la rendición de cuentas histórica y semánticamente está muy relacionada con la contabilidad (accounting), se ha ido desligando de este último concepto, ampliando su ámbito y sentido, sobre todo en aquellos países que adoptan modos de gestión provenientes

[419] Tiene que ser comunicada de forma inteligible para sus destinatarios, es decir, las personas ajenas a la organización que la suministra. Un exceso de información desorienta y obstaculiza su análisis y comprensión, de modo que, si bien con el desarrollo de las nuevas tecnologías el potencial de producción de información y estadísticas o indicadores ha aumentado exponencialmente, los ciudadanos no parecen sentirse mejor informados que antes.

del sector privado[420]. De tal forma, trasciende de lo meramente económico, y a menudo sirve como un paraguas conceptual que abarca otros conceptos distintos, tales como la transparencia, la eficiencia, la responsabilidad, el buen gobierno, etc.[421]. Aun así, en aquel ámbito han sido recurrentes las definiciones que se han dado del mismo, individualizando sus elementos esenciales, que confluyen en entender que con ella se trata de explicar y justificar la finalidad de las decisiones, acciones y omisiones del órgano, organismo o autoridad pública, así como los medios por los que se manifiesta[422].

De tal modo, se resalta su exigibilidad, bien por parte de la ciudadanía como por quien tiene encomendada su fiscalización, así como su obligatoriedad, lo que supone el derecho a obtener una respuesta y la obligación de darla y, por ello, que su incumplimiento pueda ser eventualmente sancionado. Así, comporta la necesidad de responder por la gestión pública en dos planos, pues requiere tanto informar sobre las decisiones tomadas como una explicación sobre ellas, es decir, información y justificación.

En consecuencia, la rendición de cuentas remite a la idea de responsabilidad –como instrumento para mejorar la eficacia y eficiencia de la gestión pública–, no solo frente a los órganos políticos o técnicos de fiscalización, sino también frente a los ciudadanos, lo que la vincula a la transparencia,

---

[420] Véase Bovens, M. (2007). Public Accountability. En Ferlie, E., Lynn Jr. L. E. y Pollitt C. (Eds.). *The Oxford Handbook of Public Management.* Oxford: Oxford University Press, pp. 182-183, quien señala que en la Europa continental, con una fuerte tradición de Derecho administrativo y un Estado de Derecho consolidado, ha sido por término medio menos receptivo en la adopción de estos estilos más gerenciales orientados a la gobernanza.

[421] En este sentido, Mulgan, R. (2000) "Accountability": an ever-expanding concept?. *Public Administration, 78*, *Issue 3*, pp. 555 y ss. http://doi.org/10.1111/1467-9299.00218, quien señala que el alcance y el significado de la rendición de cuentas se ha ampliado en diversas direcciones, más allá de su sentido básico de requerir a dar cuenta de lo realizado, lo que, en algunos aspectos, no es sólo una cuestión terminológica, sino también de política institucional y administrativa sobre los medios para hacerla efectiva en una democracia compleja.

[422] Hunt, G. (2006). The principle of complementarity: freedom of information, public accountability and whistleblowing. En Chapman, R. A. y Hunt, M. (Eds.) *Open government in a theorical and practicas context*. Aldershot: Ashgate Publishing, pp. 43-44.

como modo de conocer qué uso se ha hecho de los recursos públicos. Se produce así una unión[423] entre responsabilidad y transparencia, que no es sino consecuencia de la creciente exigencia de un mayor conocimiento de las más diversas cuestiones públicas. De esta manera, si el concepto de rendición de cuentas se integra en el de transparencia, pues éste se refiere a una idea más amplia de la que aquél es solo un aspecto[424], al tiempo, la transparencia es una herramienta o instrumento para la rendición de cuentas.

En nuestro ámbito jurídico-político, la rendición de cuentas no ha llegado a utilizarse de un modo generalizado, aunque es un término de uso común, como se ha manifestado con anterioridad, normalmente ligado a la

---

[423] Como señala Schedler, A. (1999). Conceptualizing Accountability. En Schedler, A., Diamond L., y Plattner, Marc F. (Eds.). *The Self-restraining state. Power and Accountability in New Democracies*, Boulder: Lynne Rienner Publishers, p. 20, la demanda de *accountability* viene originada por la opacidad del poder, ya que si éste fuera transparente no se le requeriría que rindiera cuentas.

[424] En Gran Bretaña, tanto la responsabilidad como la transparencia son principios que se deben aplicar en todos los ámbitos de la vida pública, de modo que, por el primero «los que ocupan cargos públicos son responsables de sus decisiones y acciones ante el público y deben someterse al escrutinio que sea apropiado para su cargo», mientras que por el segundo «lo que ocupan cargos públicos deben obrar de la forma más abierta posible en todas las decisiones que toman y en todas las acciones que realizan. Deberían justificar sus decisiones y limitar la información solo en el caso de que esto sea lo más necesario para el interés público». *Vid.* el documento Committee on Standards in Public Life (1995). *The 7 principles of public life.* En https://www.gov.uk/government/publications/the-7-principles-of-public-life/the-7-principles-of-public-life--2, también conocido como Informe Nolan, Patrick Nolan, M. (1996). Normas de conducta para la Vida Pública. *Documentos INAP, 9*. Los Siete Principios de la Vida Pública son: i) Desinterés. Los que ocupan cargos públicos deberían tomar decisiones sólo con arreglo al interés público; ii) Integridad. Los que ocupan cargos públicos no deberían colocarse bajo ninguna obligación financiera u otra con terceros u organizaciones que puedan influirles en el desempeño de sus responsabilidades oficiales; iii) Objetividad. Al llevar a cabo asuntos públicos, incluidos los nombramientos públicos, la contratación pública, o la recomendación de individuos para recompensas y beneficios, los que ocupan cargos públicos deberían elegir por mérito; iv) Responsabilidad. Los que ocupan cargos públicos son responsables de sus decisiones y acciones ante el público y deben someterse al escrutinio que sea apropiado para su cargo; v) Transparencia. Los que ocupan cargos públicos deberían obrar de la forma más abierta posible en todas las decisiones que toman y en todas las acciones que realizan. Deberían justificar sus decisiones y limitar la información solo en el caso de que esto sea lo más necesario para el interés público; vi) Honestidad. Los que ocupan cargos públicos tienen la obligación de declarar todos los intereses privados relacionados con sus responsabilidades públicas y de tomar medidas para solucionar cualquier conflicto que surja de tal forma que protejan el interés público; y, vii) Liderazgo. Los que ocupan cargos públicos deberían fomentar y apoyar estos principios con liderazgo y ejemplo.

contabilidad, al ámbito presupuestario o a la justificación de gastos, aunque no siempre, ya que viene utilizándose en ocasiones como una evocación o término retórico relacionado con la buena administración o buen gobierno[425], a semejanza de lo que ocurre en no pocos casos con el término «transparencia». De tal modo, en algunas normas se refiere a lo económico-contable y su fiscalización, mientras que en otras ocasiones tiene un sentido más amplio y hace referencia al resultado de las funciones desempeñadas o cometidos confiados.

De lo primero es ejemplo la Ley 47/2003[426], de 26 de noviembre, General Presupuestaria, que en el Título V sobre la contabilidad del sector público estatal, el apartado tercero del artículo 119, referido a los principios generales, dispone que las entidades que lo integran quedan sometidas a la obligación de rendir cuentas de sus operaciones, cualquiera que sea su naturaleza, al Tribunal de Cuentas. En este sentido, la Ley 7/1988, de 5 de abril. de funcionamiento del Tribunal de Cuentas, establece en su artículo 34 quiénes están obligados a rendirle cuentas de sus operaciones, con arreglo a su respectivo régimen de contabilidad. Nada se dice en estas normas, en cambio, de la transparencia pública como exigibilidad ligada a la rendición de cuentas.

De lo segundo. por su parte, es ejemplo la Ley Orgánica 4/2007, de 12 de abril, que modifica la Ley Orgánica 6/2001, de 21 de diciembre, de Universidades, y que se refiere a «la exigencia de rendir cuentas sobre el cumplimiento de sus funciones», estableciendo en su artículo 2.4 que la autonomía universitaria exige y hace posible que las Universidades rindan cuentas del uso de sus medios y recursos a la sociedad, aunque también lo emplea en el otro sentido, como el artículo 81.5, por el que las Universidades

---

425 Como en otros lugares, donde el término se ha convertido en un icono para la buena gobernanza tanto en el sector público como en el sector privado, como señala Bovens, M. (2007), op. cit. p. 4, refiriéndose a los EEUU.

426 «BOE» núm. 284, de 27/11/2003.

están obligadas a rendir cuentas de su actividad ante el órgano de fiscalización de cuentas de la Comunidad Autónoma.

Por consiguiente, podemos convenir que la idea de la rendición de cuentas se encuentra presente en nuestro sistema público, pero no está determinado el alcance y contenido que debe tener —pues debe encontrar su concreción, en cuanto obligatoriedad y exigibilidad, en las normas—, ni su conexión con la transparencia.

Siendo su finalidad la fiscalización o control en sus diversos sentidos del sector público, debe estar completamente ligada tanto al derecho de acceso a la información como a la transparencia activa, como una divulgación de interés público con un mayor alcance que la mera puesta a disposición de datos. Por tanto, desde esta perspectiva, su utilidad para nuestro sistema reside en que comporta el derecho a recibir información y la obligación correspondiente de divulgar todos los datos necesarios, e implica al tiempo el derecho a recibir una explicación y el deber correspondiente de justificar el ejercicio del poder, como forma de acotar y condicionar su discrecionalidad, pero también para exigir la responsabilidad y la interdicción de la arbitrariedad de los poderes públicos, que garantiza el artículo 9.3 CE.

En cambio, la situación actual en nuestro país es la recogida por el Tribunal Supremo en su Sentencia de 29 de mayo de 2012, cuando dice que «los ciudadanos tienen derecho –salvo en determinadas materias protegidas– a conocer la documentación recogida en los archivos y registros administrativos; pero no lo tienen a obtener explicaciones del Gobierno y la Administración sobre cualquier asunto de interés general».

2.3 La relación entre la publicidad y el principio de transparencia en la actuación de la Administración

Existe una estrecha relación entre la publicidad y el principio de transparencia. La publicidad y transparencia se necesitan mutuamente e implica un modo de actuar que facilita la participación de cualquier persona, el acceso a los procedimientos administrativos y se contrapone al secreto, a una actuación opaca de la Administración.

En un Estado democrático la actividad de la Administración cooperativa se fundamenta en la información, coordinación, garantía de seguridad y consenso, y para la consecución de esos objetivos la publicidad y transparencia son modos necesarios en la actuación de aquélla.

2.3.1 El principio general de transparencia y la publicidad

La transparencia se posibilita a través de diversas vías, tanto la que se denomina transparencia activa como la pasiva, encontrando en el ordenamiento jurídico su concreción como principio general, como obligación de publicidad y como reconocimiento del derecho de acceso.

En especial, en esta materia, la exigencia de transparencia de los poderes públicos adquiere la categoría de principio que debe guiar su actuación, pues sobre ésta se proyecta también ese principio general, plasmado desde la previsión del artículo 3.5 de la ya derogada Ley 30/1992, en la actualidad sustituida por la Ley 40/2015 LRJSP[427], por el que, en sus relaciones con los ciudadanos, las Administraciones públicas actúan de conformidad con el principio de transparencia. Perspectiva que ha sido recogida en diferentes ámbitos. Entre ellos, destacamos al ámbito económico. La Ley Orgánica 2/2012, de 27 de abril, de Estabilidad Presupuestaria y Sostenibilidad Financiera, establece algunas previsiones relacionadas con las cuentas públicas. Concretamente, su artículo 6[428], dedicado al principio de

---

[427] Véase el artículo 3.1.c) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. «BOE» núm. 236, de 02/10/2015.

[428] Artículo 6. Principio de transparencia. «1. La contabilidad de las Administraciones Públicas y demás sujetos comprendidos en el ámbito de aplicación de esta Ley, así como sus Presupuestos y liquidaciones, deberán contener información suficiente y adecuada que permita verificar su situación financiera, el cumplimiento de los objetivos de estabilidad presupuestaria y de sostenibilidad financiera y la observancia de los requerimientos acordados en la normativa europea en esta materia. A este respecto, los Presupuestos y cuentas generales de las distintas Administraciones integrarán información sobre todos los sujetos y entidades comprendidos en el ámbito de aplicación de esta ley. 2. Corresponde al Ministerio de Hacienda y Administraciones Públicas proveer la disponibilidad pública de la información económico-financiera relativa a los sujetos integrados en el ámbito de aplicación de esta Ley, con el alcance y periodicidad que se derive de la aplicación de las normas y acuerdos nacionales y de las disposiciones comunitarias. Las Administraciones Públicas suministrarán toda la información necesaria para el cumplimiento de las disposiciones de esta Ley o de las normas y acuerdos que se adopten en su desarrollo, y garantizarán la coherencia de las normas

transparencia, establece en el apartado 2 que corresponde al Ministerio de Hacienda y Administraciones Públicas, actualmente Ministerio de Hacienda y Función Pública, proveer la disponibilidad pública de la información económico-financiera relativa a los sujetos integrados en el ámbito de aplicación de esta Ley, con el alcance y periodicidad que se derive de la aplicación de las normas y acuerdos nacionales y de las disposiciones comunitarias. Además, tal y como afirma su apartado 3, igualmente estarán sometidas a disponibilidad pública las previsiones utilizadas para la planificación presupuestaria, así como la metodología, supuestos y parámetros en los que se basen. Vemos que la transparencia es un principio informador de la totalidad del ciclo presupuestario.

El primer aspecto cabría englobarlo en la rendición de cuentas de tipo horizontal, limitada a suministrar la información al órgano que puede exigirla. Aquí la transparencia no es un valor en sí misma, sino un mero auxilio para poder asegurar la efectividad del principio de estabilidad presupuestaria, de modo que sus exigencias no están dirigidas a satisfacer ninguna aspiración de los ciudadanos, sino que están concebidas como un instrumento de uso exclusivo entre Administraciones.

En el segundo, en cambio, se establece que con el fin de dar cumplimiento al principio de transparencia y a las obligaciones de publicidad derivadas de las disposiciones de la Ley, el Ministerio podrá publicar información económico-financiera de las Administraciones públicas con el alcance, metodología y periodicidad que se determine conforme a los acuerdos y normas nacionales y las disposiciones comunitarias[429]. Igualmente, el Ministerio de Hacienda y Administraciones Públicas creará una central de

---

y procedimientos contables, así como la integridad de los sistemas de recopilación y tratamiento de datos. 3. Igualmente estarán sometidas a disponibilidad pública las previsiones utilizadas para la planificación presupuestaria, así como la metodología, supuestos y parámetros en los que se basen».

[429] Artículo 27. Instrumentación del principio de transparencia. «5. Con el fin de dar cumplimiento al principio de transparencia y a las obligaciones de publicidad derivadas de las disposiciones de la Ley, el Ministerio de Hacienda y Administraciones Públicas podrá publicar información económico-financiera de las Administraciones Públicas con el alcance, metodología y periodicidad que se determine conforme a los acuerdos y normas nacionales y las disposiciones comunitarias».

información, de carácter público, que provea de información sobre la actividad económico-financiera de las distintas Administraciones Públicas[430].

En relación a las diferentes instancias territoriales, destacar el interés de la diferenciación que realiza esta última norma entre información a la ciudadanía, transparencia en la gestión y transparencia política. Así, por la primera la Administración pública autonómica y su sector público instrumental tienen que garantizar a la ciudadanía el derecho a la información administrativa, como primer peldaño del concepto de acceso, y, en general, el derecho a tener información y a conocer las actuaciones y las iniciativas de actuación pública que emprende en virtud del ejercicio de sus competencias y los servicios públicos que ofrece. En cuanto a la transparencia en la gestión, dispone que en todos los procesos de gestión se actuará bajo el principio de transparencia y se hará pública toda la información que la Ley permita, especialmente la manera de hacer publicidad de ésta y de facilitar su acceso a la ciudadanía. Esta transparencia se observará principalmente en la adjudicación y la ejecución de los contratos, en la firma de convenios de colaboración, tanto los suscritos con otras administraciones públicas como con entidades privadas, y en la concesión de ayudas y subvenciones. Finalmente, la transparencia política se define como el nivel de accesibilidad y publicidad que el Gobierno ofrece a la ciudadanía en relación con sus actividades públicas y la garantía del ejercicio del derecho de los ciudadanos y de las ciudadanas a la información sobre el funcionamiento interno del Gobierno y sus instituciones, como también de todos los aspectos que afectan a la gestión política. Para alcanzar la transparencia política, es necesario establecer medidas de prevención y control de conflictos de intereses y medidas de información pública y de registro de actividades, bienes y derechos de los altos cargos de la administración y del Gobierno.

Contar con más información, de mejor calidad y accesible mitiga los problemas de información asimétrica y disipa incertidumbres sobre el

[430] Véase el artículo 28.1 del mismo texto normativo.

funcionamiento de las Administraciones públicas españolas, pues permite un seguimiento más riguroso de su situación económica y financiera

2.3.2 La publicidad y transparencia como premisas de una actuación democrática de la Administración

La publicidad y transparencia ofrecen la garantía de una Administración abierta y ponderada. Estos dos principios implican que la actuación de la Administración se llevará a cabo bajo la observación y vigilancia de los particulares y el público en general.

En un Estado democrático y de Derecho existe la idea básica del establecimiento de controles como límite en el ejercicio del poder, pero visto desde una perspectiva dinámica, no estática.

En este sentido, que la actuación de la Administración se lleve a cabo con publicidad y transparencia puede mejorar la salvaguardia y realización efectiva de los derechos fundamentales, el cumplimiento de las exigencias que plantean a la Administración los principios del Estado de Derecho o el Estado Social, o bien una mayor eficiencia en el desempeño de los objetivos a los que la sociedad de la información somete a la Administración.

Tomando, en primer lugar, como referencia el significado que la publicidad y transparencia tienen para la efectiva realización de los derechos fundamentales, el derecho del artículo 20.1.d) CE, entendido como derecho a recibir información y a ser informado, se encuentra vinculado con el derecho de acceso de los ciudadanos a los archivos y registros administrativos, recogido en el artículo 105 b) CE.

El derecho fundamental del artículo 20.1 d) no se limita al derecho del ciudadano a ser informado a través de los diversos medios de comunicación, sino que incluye el derecho a acceder a la información que detentan los poderes públicos, incluida la Administración. El acceso a la información del ciudadano, que implica la ampliación de sus posibilidades de desarrollo personal y socioeconómico, se vincula con la información que detenta la Administración y cómo ésta la transmite. En este contexto, la publicidad y transparencia en la actuación de la Administración potenciará sus

posibilidades en la transmisión de la información al ciudadano, lo que pone de manifiesto que ambos principios son condición necesaria del ejercicio del derecho fundamental a recibir información que aquél detenta.

En segundo lugar, debe ponerse de relieve que la publicidad y transparencia son elementos esenciales para el mandato del principio del Estado de Derecho (artículo 1.1 CE). En efecto, para aquellas personas que se relacionan con la Administración esos principios significan un medio de protección. El monopolio sobre la información significa poder, por lo que un acceso a la información por medio de la publicidad y transparencia equilibra la asimetría en el ejercicio del poder y es un medio de control del ciudadano sobre los poderes públicos, y en concreto de la Administración. Que se identifique a las autoridades bajo cuya responsabilidad se tramita un procedimiento[431] es un medio de transparencia y garantiza que se produce una personalización de la responsabilidad, lo cual es un medio de racionalización y mejora de la resolución, y para el ciudadano aumenta la previsibilidad y seguridad, lo que refuerza el principio del Estado de Derecho.

Asimismo, la motivación de los actos administrativos[432] se vincula con la objetividad, imparcialidad y publicidad en la actuación de la Administración[433], e introduce previsibilidad y transparencia en su actuación.

---

[431] Artículo 53.1.b) Ley 39/2015 LPACAP.

[432] Artículo 35 Ley 39/2015 LPACAP.

[433] En este sentido se manifiesta Fernando Pablo, M.: (1993) *La motivación del acto administrativo*, Madrid: Tecnos, pp. 151 y ss.

3 LA EXIGENCIA DE UNA ADMINISTRACIÓN TRANSPARENTE EN LA PERSPECTIVA DEL ESTADO DE DERECHO.

3.1 Aparición y difusión de la transparencia como principio rector de la modernización del Estado

En el continente europeo, el libre acceso a la información fue objeto de leyes tempranas en Suecia, y en Francia[434]. La apertura de las administraciones europeas es un fenómeno que surgió solo de manera amplia en los años noventa del siglo pasado.

Pocos años más tarde, la Unión Europea «descubrió» el principio de transparencia como una vía de disminuir la creciente distancia entre las instituciones europeas y los ciudadanos europeos. Antes ya había promovido el acceso de los ciudadanos a la información en los Estados miembros, especialmente en materia de medio ambiente[435] fue en muchos Estados el punto inicial para desarrollar una cultura administrativa más abierta. Al mismo tiempo, la exigencia de más transparencia formaba parte de programas de modernización orientados a una administración cooperativa y una mayor participación de los ciudadanos.

3.1.1 Desarrollo al nivel nacional

El punto de partida para la realización de una administración transparente o abierta, ha sido la posibilidad del acceso a la información, particularmente a los documentos, los archivos y registros de los cuales dispone la Administración Pública.

---

[434] Ley núm. 78-753, de 17 de julio de 1978, por la que se establecen diversas medidas para la mejora de las relaciones entre la Administración y el público, así como diversas disposiciones de orden administrativo, social y fiscal.

[435] La Directiva 90/313/CEE del Consejo, de 7 de junio de 1990, sobre libertad de acceso a la información en materia de medio ambiente Diario Oficial núm L 158 de 23/06/1990 p. 0056 - 0058

Esta función del acceso a la información para la implementación de los principios más generales ya destaca en las primeras leyes relevantes de los años noventa. Por lo que respecta a nivel nacional, el apartado quinto de la Exposición de Motivos de la Ley 30/1992 hacía alusión a «las nuevas corrientes de la ciencia de la organización aportan un enfoque adicional en cuanto mecanismo para garantizar la calidad y transparencia de la actuación administrativa», y en el noveno a la ruptura con «la tradicional opacidad de la Administración». Los artículos encargados de romper con la misma, eran los artículos del 35 al 37 de aquella.

El avance esencial alcanzado por esta legislación lo constituye la introducción del acceso de los particulares a los documentos oficiales como regla general, debiéndose justificar todo rechazo de dar acceso a informaciones.

Para la implementación del derecho de libre acceso a la información se han creado, en algunos países, comisionados que velan sobre el cumplimiento de los derechos de acceso de los particulares. Puesto que las decisiones sobre el acceso a la información tienen que tomar en consideración aspectos de protección de datos, parece razonable integrar ambas funciones. Así, tanto en el Reino Unido como en Alemania se han configurado las dos funciones en una misma institución: el Comisionado de Información y el Comisionado para la Protección de Datos y la Libertas de Información, respectivamente.

3.1.2 La transparencia en el sistema multinivel

El derecho y la política de información de las instituciones europeas siguen dando impulsos para el mejoramiento de la transparencia administrativa a nivel nacional.

Destaca SOMMERMANN[436] como medidas importantes la Decisión del Consejo de 20 de diciembre de 1993, relativa al acceso del público a los documentos del Consejo[437], y la inserción del derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión en el Derecho primario, a través del Tratado de Ámsterdam de 1997[438], con la subsiguiente concretización por el Reglamento (CE) núm. 1049/2001[439]. La facilitación del acceso a la información en la Unión Europea ganó una importancia creciente dentro de la política de apertura de la Comisión como una estrategia de acercar los ciudadanos a las instituciones de la Unión Europea[440].

No obstante, este intento no tuvo un gran éxito. El principio de transparencia se realizó a través de una política abierta de información de la mayoría de las instituciones de la Unión, lo que contrastaba con el comportamiento de algunos gobiernos nacionales.

Sin embargo, el principio de transparencia pertenece al acervo comunitario, y tiene el respaldo de todos los Estados miembros de la Unión. Esto se manifiesta en el hecho de que aparece explícitamente tanto en el Tratado de la Unión Europea[441], como en el Tratado de Funcionamiento de la Unión

---

[436] Sommermann, K. P. (2010). La exigencia de una Administración transparente en la perspectiva de los principios de democracia y del Estado de Derecho. En García Macho, R. (Ed.), *Derecho administrativo de la información y administración transparente*. Madrid: Marcial Pons. p. 16.

[437] Decisión 93/731/CE (DO, núm. L 340, de 31 de diciembre de 1993, p.43)

[438] DO, núm C340, de 10 de noviembre de 1997, p. 3.

[439] DO, núm L. 145, de 31 de mayo de 2001, p. 43.

[440] Este esfuerzo por parte de la Comisión se vio sintetizado en el Libro Blanco de 2001 sobre «La gobernanza europea» COM (2001) 428 final. El programa para mejorar la transparencia fue desarrollado en el Libro Verde «Iniciativa europea a favor de la transparencia» COM (2006) 194 final.

[441] «Artículo 11. 1. Las instituciones darán a los ciudadanos y a las asociaciones representativas, por los cauces apropiados, la posibilidad de expresar e intercambiar públicamente sus opiniones en todos los ámbitos de actuación de la Unión. 2. Las instituciones mantendrán un diálogo abierto, transparente y regular con las asociaciones representativas y la sociedad civil. 3. Con objeto de garantizar la coherencia y la transparencia de las acciones de la Unión, la Comisión Europea mantendrá amplias consultas con las partes interesadas. 4. Un grupo de al menos un millón de ciudadanos de la Unión,

Europea[442]. De igual modo, el Tratado de Lisboa ha mantenido a este respecto la línea del Tratado constitucional.

3.1.3 La transparencia como principio y obligación

La transparencia se configura en algunos supuestos como un mandato positivo para la difusión de la información. La legislación ha configurado en determinadas ocasiones la obligación de la Administración Pública de dar publicidad a sus actuaciones o a su funcionamiento[443].

---

que sean nacionales de un número significativo de Estados miembros, podrá tomar la iniciativa de invitar a la Comisión Europea, en el marco de sus atribuciones, a que presente una propuesta adecuada sobre cuestiones que estos ciudadanos estimen que requieren un acto jurídico de la Unión para los fines de la aplicación de los Tratados. Los procedimientos y las condiciones preceptivos para la presentación de una iniciativa de este tipo se fijarán de conformidad con el párrafo primero del artículo 24 del Tratado de Funcionamiento de la Unión Europea». DOUE núm. C 326 de 26/10/2012 p. 0013 - 0045 (Versión consolidada)

[442] «Artículo 15 (antiguo artículo 255 TCE) 1. A fin de fomentar una buena gobernanza y de garantizar la participación de la sociedad civil, las instituciones, órganos y organismos de la Unión actuarán con el mayor respeto posible al principio de apertura. 2. Las sesiones del Parlamento Europeo serán públicas, así como las del Consejo en las que éste delibere y vote sobre un proyecto de acto legislativo. 3. Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte, con arreglo a los principios y las condiciones que se establecerán de conformidad con el presente apartado. El Parlamento Europeo y Consejo, con arreglo al procedimiento legislativo ordinario, determinarán mediante reglamentos los principios generales y los límites, por motivos de interés público o privado, que regulan el ejercicio de este derecho de acceso a los documentos. Cada una de las instituciones, órganos u organismos garantizará la transparencia de sus trabajos y elaborará en su reglamento interno disposiciones específicas sobre el acceso a sus documentos, de conformidad con los reglamentos contemplados en el párrafo segundo. El Tribunal de Justicia de la Unión Europea, el Banco Central Europeo y el Banco Europeo de Inversiones sólo estarán sujetos al presente apartado cuando ejerzan funciones administrativas. El Parlamento Europeo y el Consejo garantizarán la publicidad de los documentos relativos a los procedimientos legislativos en las condiciones establecidas por los reglamentos contemplados en el párrafo segundo». DOUE núm. C 326 de 26/10/2012 p. 0047 - 0390 (Versión consolidada)

[443] Señala Pitschas, R. (2006). El Derecho administrativo de la información. La regulación de la autodeterminación informativa y el gobierno electrónico», en Barnés Vázquez, J. (Coord). *Innovación y reforma en el Derecho administrativo*, Sevilla: Derecho Global, p. 260, esta tarea requiere además la garantía del acceso de todos a las infraestructuras informativas y a las redes, acceso que debe garantizar la Administración, asegurando un nivel o estándar mínimo de información.

3.1.3.1 Principio democrático y transparencia

Entre sus diversos aspectos, la transparencia incorporada al principio democrático comporta también la exigencia de una mayor participación, dando entrada a los ciudadanos en la elaboración de las decisiones que les afecten.

De tal modo, la transparencia sirve igualmente para la consecuencia de esa otra finalidad constitucional, posibilitando la efectividad del genérico principio de participación a que alude el apartado segundo del artículo 9[444] de la Constitución Española, o la información y participación de las organizaciones que los representan en los procesos decisorios que les afecten, por ejemplo, el artículo 51 de aquella[445].

Esa acción positiva de permitir la participación comporta una trasmisión hacia los ciudadanos de la información que se utiliza en las organizaciones

---

[444] Artículo 9 de la Constitución española. «2. Corresponde a los poderes públicos promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social».

[445] Artículo 51 de la Constitución española. «1. Los poderes públicos garantizarán la defensa de los consumidores y usuarios, protegiendo, mediante procedimientos eficaces, la seguridad, la salud y los legítimos intereses económicos de los mismos. 2. Los poderes públicos promoverán la información y la educación de los consumidores y usuarios, fomentarán sus organizaciones y oirán a éstas en las cuestiones que puedan afectar a aquéllos, en los términos que la ley establezca. 3. En el marco de lo dispuesto por los apartados anteriores, la ley regulará el comercio interior y el régimen de autorización de productos comerciales». Para García de Enterría Martínez-Carande, E. (1989). Principio y modalidades de la participación ciudadana en la vida administrativa. En Gómez-Ferrer Morant, R. (coord.). *Libro homenaje al profesor José Luis Villar Palasí*. Madrid: Civitas, pp. 441 y ss., con ello se puede romper la impermeabilidad que muchas veces reviste a los agentes administrativos con respecto al ámbito económico-social en el que actúan, intentando que en el proceso de adopción de las decisiones de la administración se tengan en cuenta el interés y los puntos de vista del sector involucrado en ellas. No en balde, como ha entendido Bermejo Vera, J. (1993). La participación de los administrados en los órganos de la Administración Pública. En *La protección jurídica del ciudadano. Estudios en homenaje al profesor Jesús González Pérez, Tomo I*. Madrid: Civitas, p. 641, la razón de su reconocimiento puede estribar en que el acierto de las decisiones administrativas aumenta cuando los propios destinatarios de las mismas participan en la conformación de las decisiones y métodos elegidos para llegar a ellas.

públicas, posibilitando su conocimiento público, e integrar los diferentes intereses que pueden revelarse.

En términos generales, la cantidad y el contenido de la información que suministran los poderes públicos a la sociedad, es decir, la forma en que realizan su actividad de comunicación o información, tiene un papel de primer orden para el buen funcionamiento de un sistema democrático. Ello, por cuanto solo con transparencia se podrá posibilitar un control democrático de la actividad administrativa, sobre su desarrollo y adecuación con el interés público y a la legalidad, constituyéndose así en una pieza necesaria para ejercer la facultar de decidir, de participar en los asuntos públicos en los términos del artículo 23.1 CE, bien directamente, bien a través de representantes.

En consecuencia, puede entenderse que existe una obligación de los poderes públicos de suministrar a los ciudadanos toda aquella información que les permita conocer y valorar lo realizado por quienes los representan, conocimiento que no hará sino legitimar aún más el ejercicio de sus funciones[446].

3.1.4 El acceso a la información por los ciudadanos

3.1.4.1 Naturaleza jurídica

La transparencia administrativa comporta el derecho de los ciudadanos a informarse, como modo de hacerla efectiva. El acceso a la información administrativa ha ido experimentando un progreso positivo, de modo que, aunque no se contemple en la Constitución Española expresamente como tal, puede considerarse que en ésta se encuentran los datos necesarios para garantizarlo. Su interpretación dinámica se debe considerar clave para lograr una completa efectividad del mismo.

---

[446] En esta línea, señala Sáinz Moreno, F. (2004). Secreto y transparencia. En Sáinz Moreno, F. (Dir.). *Estudios para la reforma de la Administración Pública.* Madrid: INAP. pp. 166 y ss. que la democracia exige un incesante proceso hacia la máxima transparencia de la Administración, con los límites necesarios.

Recogido en el artículo 105 b) CE, dispone que la Ley regulará, entre otras materias, «el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas».

En cualquier caso, la transparencia no es, ni comporta, ningún derecho fundamental. Así se han pronunciado expresamente, tanto la jurisprudencia[447], como la doctrina mayoritaria[448].

Sin embargo, en ocasiones el acceso a la información, manifestación de la transparencia, se encuentra relacionado con otros derechos que sí son fundamentales. Es el caso del nexo entre el derecho de acceso y la libertad de información reconocida constitucionalmente, entendiéndose la libertad de información en el sentido de libertad de recibir información veraz por cualquier medio de difusión [artículo 20.1.d) CE][449]. Sin embargo, tanto la

---

[447] Véase, entre otras, las SSTS de fecha 30 de enero de 1989; 30 de marzo de 1999; y 19 de junio de 2012. Esta última expresamente declara en su Fundamento Jurídico 1 que «[…] se reconduce a precepto constitucional, como el artículo 105 CE*, que no tiene la consideración de derecho fundamental o libertad pública, de los fijados en el* artículo 53.2 CE», y su Fundamento Jurídico 2 « No obstante lo anterior, compartimos la tesis de la Sala de instancia cuando niega que esta irregularidad o vicio sea susceptible de configurar una pretensión que pueda tener cabida en el limitado objeto del especial proceso contencioso-administrativo al que acudió el recurrente puesto que ni tal derecho de acceso a la información contenida en los archivos y registros constituye, en sí mismo, un derecho fundamental de los que se pueden hacer valer en dicho proceso […]».

[448] Vid., sobre las distintas posturas sobre su naturaleza, Fernández Ramos, S. (2013). *El acceso a la información en el Proyecto de Ley de Transparencia, acceso a la información pública y buen gobierno*. Zaragoza: IAAP, pp. 329-330, y sobre la consideración del derecho de acceso a la información como derecho fundamental, Sánchez de Diego Fernández de la Riva, M. (2008). Un derecho fundamental a acceder a la información pública. *El derecho de acceso a la información pública Actas del Seminario Internacional Complutense 27 -28 junio 2007*. Madrid: CERSA, pp. 31 y ss.

[449] Para Pasquier, M. y Villeneuve, J. P. (2007). Organizational barriers to transparency: a typology and analysis of organizational behavior tending to prevent or restrict access to information. *International Review of Administrative Sciences*, *73, p. 148*. http://doi.org/10.1177/0020852307075701, la transparencia se base en el innegociable derecho a saber recogido de forma explícita en el artículo 19 de la Declaración Universal de los Derechos Humanos, por el que «todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión».

doctrina como la jurisprudencia han apreciado dificultades en mantener esta postura, desde la perspectiva de que el derecho del referido artículo 20.1 d) no trataría la información en el sentido del acceso a la información administrativa como derecho de los ciudadanos[450]. En este sentido, el Tribunal Supremo[451] afirma que no debe confundirse el derecho constitucional de información con el derecho de los ciudadanos a tener acceso a los archivos y registros administrativos, aun reconociendo trascendencia de dicho derecho en un sistema democrático, y la conexión del artículo 20.1. d) con el artículo 105 b).

3.1.4.2 El derecho de acceso a la información administrativa

El apartado d) del artículo 13 LPACAP[452] remite al contenido de la LTBG en todo lo relacionado con el acceso a la información de los ciudadanos en sus relaciones con las Administraciones Públicas. Por tanto, el derecho así configurado debe considerarse como un derecho subjetivo de todo ciudadano. No obstante, el Tribunal Supremo[453] ha declarado que este derecho general de acceso a la información de todos los ciudadanos es diferente de aquél reconocido a los interesados en un procedimiento en concreto ya iniciado y pendiente de resolución o resuelto por la Administración, regulado en el apartado a) del artículo 53.1 LPACAP[454]. En

---

[450] Vid., entre otros Mestre Delgado, J.F. (1998). *El derecho de acceso a archivos y registros administrativos [análisis del artículo 105.b) de la Constitución]* (2ª edición ampliada). Madrid: Civitas pp. 96 y ss., y Díez Sánchez J. J. (1999). *Razones de Estado y Derecho*. Valencia: Tirant lo Blanch, pp. 188 y ss.

[451] Sentencia del Tribunal Supremo de 19 de mayo de 2003.

[452] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE núm. 236, de 2 de octubre de 2015 Artículo 13. Derechos de las personas en sus relaciones con las Administraciones Públicas. «Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos: […] d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico».

[453] Sentencia del Tribunal Supremo de 30 de marzo de 1999.

[454] Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE núm. 236, de 2 de octubre de 2015 Artículo 53. Derechos del interesado en el

este sentido, tampoco el derecho de acceso a información sobre los propios datos que recoge la LOPD, cabrá reconducirlo a la transparencia, al requerir una cualificación especial.

Se trata, en cambio, del derecho que asiste al ciudadano que se halla en el trance previo de reunir información necesaria para tomar conocimiento de su situación y derechos frente a los poderes públicos. Por tanto, no se exige requisito alguno general de orden legitimados para poder obtener información más que ostentar la cualidad de ciudadano. En consecuencia, la forma de su ejercicio la establece la Ley 19/2013, de 9 de diciembre, LTBG.

3.2 Las funciones de la transparencia administrativa

3.2.1 Fortalecimiento del principio democrático

La posibilidad de informarse directamente sobre las actuaciones y motivos del poder legislativo, así como de los poderes ejecutivo y judicial, constituye un elemento importante para la formación democrática de la opinión y de la voluntad. Sin conocimiento de las responsabilidades de los actores y de sus criterios de actuación el control democrático queda incompleto o inoperable. La claridad de la atribución de responsabilidades tanto entre los poderes públicos como entre los órganos de cada uno de ellos constituye una condición para hacer visible la responsabilidad política.

---

procedimiento administrativo. «1. Además del resto de derechos previstos en esta Ley, los interesados en un procedimiento administrativo, tienen los siguientes derechos: a) A conocer, en cualquier momento, el estado de la tramitación de los procedimientos en los que tengan la condición de interesados; el sentido del silencio administrativo que corresponda, en caso de que la Administración no dicte ni notifique resolución expresa en plazo; el órgano competente para su instrucción, en su caso, y resolución; y los actos de trámite dictados. Asimismo, también tendrán derecho a acceder y a obtener copia de los documentos contenidos en los citados procedimientos. Quienes se relacionen con las Administraciones Públicas a través de medios electrónicos, tendrán derecho a consultar la información a la que se refiere el párrafo anterior, en el Punto de Acceso General electrónico de la Administración que funcionará como un portal de acceso. Se entenderá cumplida la obligación de la Administración de facilitar copias de los documentos contenidos en los procedimientos mediante la puesta a disposición de las mismas en el Punto de Acceso General electrónico de la Administración competente o en las sedes electrónicas que correspondan».

3.2.2 Aseguramiento del principio del Estado de Derecho

La división de poderes, entendida como un sistema basado en *checks and balances* para impedir una concentración de poderes, solo puede cumplir su función controladora si existen estructuras institucionales que permitan identificar los actores responsables y si el comportamiento y los actos a controlar no quedan en la oscuridad. En la medida que se quiere movilizar al ciudadano para el control, hay que proporcionarle los instrumentos necesarios de información. La claridad de la atribución de responsabilidades es igualmente crucial para la realización de un Estado de Derecho.

Una ampliación de la transparencia, respetando los derechos individuales, fortalece la confianza en la racionalidad y objetividad de la actuación administrativa, criterios de un Estado de Derecho que de esta manera gana en legitimación. Una comunicación más abierta de la Administración Pública con los ciudadanos, ofrece al mismo tiempo una oportunidad para la Administración de completar su saber y de conseguir informaciones que pueden ser útiles para el desarrollo de sus proyectos.

3.3 Sujetos obligados y derecho de acceso

Los sujetos a los que se refiere el artículo 3[455] no están sujetos al deber de atender el derecho de acceso, pues no se les aplica el capítulo III del título I de la Ley 19/2013, de 9 de diciembre, LTBG.

La información respecto de la que cabe solicitar el acceso en relación con la Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional y el Consejo General del Poder Judicial, así como el Banco de España, el Consejo de Estado, el Defensor del Pueblo, el Tribunal

[455] «Artículo 3. Otros sujetos obligados. Las disposiciones del capítulo II de este título serán también aplicables a: a) Los partidos políticos, organizaciones sindicales y organizaciones empresariales. b) Las entidades privadas que perciban durante el período de un año ayudas o subvenciones públicas en una cuantía superior a 100.000 euros o cuando al menos el 40 % del total de sus ingresos anuales tengan carácter de ayuda o subvención pública, siempre que alcancen como mínimo la cantidad de 5.000 euros».

de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas, es solo la que tenga que ver con sus actividades sujetas al derecho administrativo[456]. Contra las resoluciones dictadas por estos órganos, solo cabe la interposición de recurso contencioso-administrativo, de modo que no es posible la impugnación ante el Consejo de Transparencia y Buen Gobierno[457].

Por otro lado, la disposición adicional octava de la Ley, faculta al Congreso de los Diputados, al Senado y a las Asambleas Legislativas de las Comunidades Autónomas para contar con una regulación propia que determine los detalles del ejercicio del derecho de acceso, pues se les reconoce la posibilidad de que regulen en sus respectivos reglamentos la aplicación concreta de las disposiciones de la Ley.

3.4 Concepto de información pública

La definición de información pública nos la ofrece el artículo 13 de la propia Ley 19/2013, en los siguientes términos:

> *«Se entiende por información pública los contenidos o documentos, cualquiera que sea su formato o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones».*

Se considera información no solo el soporte (el documento en términos tradicionales) sino el contenido del mismo, al margen de cuál sea el formato

---

[456] Véase el Artículo 2.1 f) de la Ley 19/2013, de 9 de diciembre.

[457] Así se declara en la Ley 19/2013, de 9 de diciembre, tanto en el segundo apartado del artículo 23 «contra las resoluciones dictadas por los órganos previstos en el artículo 2.1.f) sólo cabrá la interposición de recurso contencioso-administrativo», como en el segundo párrafo del apartado primero de la disposición adicional cuarta «contra las resoluciones dictadas por las Asambleas Legislativas y las instituciones análogas al Consejo de Estado, Consejo Económico y Social, Tribunal de Cuentas y Defensor del Pueblo en el caso de esas mismas reclamaciones sólo cabrá la interposición de recurso contencioso-administrativo».

o soporte. Lo que, además, debe ponerse en relación con el artículo 16[458] del mismo texto legal, por el que se reconoce el acceso parcial a la información.

Hemos visto que el artículo 13 extiende el concepto de información a toda la que «obre en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título», pero de inmediato añade in fine «y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones». Es decir, parece exigir, no solo que la información esté en poder del sujeto obligado, sino que éste sea quien la haya elaborado o adquirido. Afirma el profesor PIÑAR MAÑAS que no parece acertado que la Ley haya optado por recoger la llamada "regla del autor"[459]. Parece dejar fuera la información que puede

---

[458] Artículo 16. Acceso parcial. «En los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida».

[459] La "regla del autor" aparece definida en la Sentencia del Tribunal de Primera Instancia (Sala Quinta ampliada), de 30 de noviembre de 2004, IFAW Internationaler Tierschutz-Fonds gGmbH contra Comisión, asunto T-168/02. Tal y como afirma el § 53 de la Sentencia, «antes de la entrada en vigor del Reglamento [el Tribunal se refiere al Reglamento (CE) 1049/2001, del Parlamento Europeo y del Consejo de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión], el acceso del público a los documentos de la Comisión estaba regulado por la Decisión 94/90. Su artículo 1 adoptaba formalmente el Código de conducta aprobado por el Consejo y la Comisión el 6 de diciembre de 1993, relativo al acceso del público a los documentos del Consejo y de la Comisión (DO 1993, L 340, p. 41; en lo sucesivo, «Código de conducta»), anexo a dicha Decisión. El Código de conducta establecía, bajo el título «Tramitación de las solicitudes iniciales», que «cuando el autor del documento que posea la Institución sea una persona física o jurídica, un Estado miembro, otra Institución u órgano comunitario, o cualquier otro organismo nacional o internacional, la solicitud deberá dirigirse directamente al mismo» (en lo sucesivo, «regla del autor»). Por lo tanto, con arreglo a la regla del autor, una institución no estaba facultada para divulgar los documentos originarios de una amplia categoría de terceros, que incluía entre otros a los Estados miembros, y el solicitante de acceso estaba obligado, en su caso, a dirigirse al tercero en cuestión». El texto completo de la Sentencia accesible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62002TJ0168&from=ES De igual modo, la Decisión de la Comisión de 8 de febrero de 1994 sobre el acceso del público a los documentos de la Comisión se puede consultar en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31994D0090&from=EN

estar en posesión de un sujeto obligado, pero que ni ha sido elaborado ni ha sido adquirido por él[460].

Sin embargo, ni el Convenio 205 del Consejo de Europa sobre Acceso a Documentos Oficiales[461], ni el Reglamento (CE) 1049/2001, del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión[462] acogen esta «regla de autor». Ahora bien, en caso de documentos originarios de terceros, las instituciones deben consultarles antes de conceder el acceso, al objeto de verificar si son o no aplicables las excepciones previstas en los apartados 1 y 2 del artículo 4 del Reglamento, salvo que se deduzca con claridad que se ha de permitir o denegar la divulgación de los mismos[463].

El acceso parcial aparece regulado en el artículo 16 de la Ley en los siguientes términos:

> *«En los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información*

---

460 Piñar Mañas, J. L. (2014). Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno. *Revista catalana de dret públic, 49, p. 10*. En http://revistes.eapc.gencat.cat/index.php/rcdp/article/download/10.2436-20.8030.01.29/n49-pinar-es.pdf

461 Véase la definición que nos ofrece la letra b) del apartado 2 del artículo primero del Convenio «"official documents" means all information recorded in any form, drawn up or received and held by public authorities». Por "documentos públicos" debemos entender toda información registrada de cualquier forma [archivada], elaborada o recibida, y en posesión de las autoridades públicas.

462 La letra a) del artículo 3 nos ofrece la definición del término "documento" como «todo contenido, sea cual fuere su soporte (escrito en versión papel o almacenado en forma electrónica, grabación sonora, visual o audiovisual) referentes a temas relativos a las políticas, acciones y decisiones que sean competencia de la institución».

463 Véase el apartado 4 del artículo 4 del Reglamento 1049/2001, del Parlamento Europeo y del Consejo, de 30 de mayo.

distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida».

Este artículo coincide con el contenido de la regulación del acceso parcial previsto en el artículo 4.6 del Reglamento 1049/2001, del Parlamento Europeo y del Consejo, de 30 de mayo, al declarar que cuando se solicite el acceso a un documento y sean aplicables a parte del mismo algunas de las excepciones previstas en su articulado, deberán divulgarse las demás partes no sometidas a dichas excepciones[464].

3.5 La naturaleza jurídica del Derecho de Acceso y el conflicto con otros derechos e intereses

Una de las cuestiones que más debate suscita es, sin duda, la relativa a la naturaleza jurídica del derecho de acceso a la información pública.

En el nuevo texto el legislador ha optado finalmente por una construcción del derecho de acceso anclado en el artículo 105.b) CE, es decir, desarrollando una concepción limitada de este, como derecho de configuración legal.

Esta alternativa ha condicionado el régimen de protección aplicable ante eventuales vulneraciones, privándole de las garantías específicas y reforzadas de las que disfrutan los derechos de naturaleza fundamental.

Solo una construcción del derecho de acceso a la información desde la óptica de los ciudadanos, reconociendo su naturaleza fundamental, contribuye a que el principio de publicidad sea, como efectivamente debe ser en un sistema democrático, la regla general y no la excepción, como en la práctica ocurre.

La inercia de nuestro sistema (pese a lo que pudiera parecer si contemplamos la multiplicidad de manifestaciones del reconocimiento del

---

[464] El artículo 4.6 del Reglamento 1049/2001 expresamente declara que «en el caso de que las excepciones previstas se apliquen únicamente a determinadas partes del documento solicitado, las demás partes se divulgarán».

principio de publicidad) es, sin embargo, más proclive a la opacidad que a una verdadera apertura informativa o «cultura de la transparencia», que pretende instaurar esta nueva Ley.

Ciertamente la LTBG supone un fuerte avance y un cambio de mentalidad, pero conserva la tendencia a considerar la transparencia como un mero principio de actuación de las Administraciones públicas, y no tanto como un verdadero derecho ciudadano.

Sea como fuere, el reconocimiento o la mera declaración de su naturaleza fundamental por su estrecha vinculación con los derechos fundamentales a la información [artículo 20.1.d) CE] y al derecho a la participación de los ciudadanos en los asuntos públicos (artículo 23 CE) no habría comportado, como tampoco ocurre con los demás derechos fundamentales, un radio de acción ilimitado[465]. Sin embargo, sí habría colocado a este derecho en mejor posición de cara a la solución de un eventual conflicto con el resto de intereses públicos y privados que, como hemos visto, pueden actuar de límite, particularmente la protección de la intimidad a través de la protección de los datos personales.

---

[465] En este sentido, por ejemplo, la SAN de 25 de febrero de 2013 (Sala de lo Contencioso-Administrativo, Sección 1ª) reconoce que «esta Sala ha venido ponderando en numerosas sentencias la protección de datos y el derecho de información, para determinar, de acuerdo con el artículo 9 de la Directiva 95/46 cuándo resultan admisibles limitaciones al derecho a la protección de datos para la libertad de expresión e información. Hemos declarado, que en esa ponderación se debe considerar la relevancia de la noticia que puede ayudar a formar la opinión pública, así como la proyección pública del particular del que se da la información […] de forma que, según hemos venido declarando en esta Sentencia, la intromisión en los derechos fundamentales de terceros resultante del ejercicio de la libertad de información sólo será legítima en la medida en que la afectación de dichos derechos resulte adecuada, necesaria y proporcionada para la realización constitucional del derecho a la libertad de información. Asimismo, esta Sala ha declarado, en la Sentencia de la Audiencia Nacional de 16 febrero 2007, que el derecho a la libertad información veraz no es un derecho absoluto y ante la ponderación de ambos derechos fundamentales, se colige que no puede en modo alguno prevalecer el derecho a la información veraz invocado sobre el derecho a protección de datos. Así, en ese caso, la publicación del nombre, apellido, DNI, domicilio, profesión y actividad asociativa de un miembro de la guardia civil, no puede ampararse en modo alguno en la finalidad invocada, pues pudo perfectamente informarse sobre la fundación de la asociación sin necesidad de proporcionar los datos personales».

Una concepción del derecho de acceso como mero derecho de configuración legal le coloca en una posición más débil a la hora de solucionar una posible colisión, por ejemplo, con el derecho a la protección de datos personales, lo que es resultado del superior rango que a este último le confiere su carácter fundamental.

3.6 Los límites del derecho de acceso a la información pública

Aunque este punto será objeto de una explicación más profunda, creo necesario apuntar unas pinceladas de una de las cuestiones centrales del derecho de acceso, como es la fijación de sus límites o excepciones.

3.6.1 Planteamiento: Transparencia y Confidencialidad

Declara LAGUNA DE PAZ, y no admite discusión alguna, que la información confiere una buena dosis de poder a quien la detenta, y que la información siempre ha sido un instrumento de gobierno[466]. En este sentido, la superación de un sistema de información pública marcado por el secretismo y, a veces, incluso por la opacidad, en favor de un sistema de transparencia, supone por tanto un desplazamiento del poder de control y decisión en favor de los ciudadanos

En un Estado democrático de Derecho la publicidad sirve, con carácter general, para alcanzar la transparencia que permite que los ciudadanos pueden visibilizar el funcionamiento de las Administraciones y, en general, el ejercicio del poder público, lo que cumple, en primer término, una misión evidente: la de permitir el control de dicha actividad y su sometimiento a la legalidad limitando la arbitrariedad, exigencia consustancial al Estado de Derecho. La transparencia, por tanto, desplaza hacia el lado de los ciudadanos buena dosis del poder que lleva implícito la información

[466] *Vid.* Laguna De Paz, J. C. (2010). Principio de confidencialidad. En Santamaría Pastor, J. A. (Dir.). *Los principios jurídicos del Derecho Administrativo.* Madrid: La Ley, pp. 1208 y 1209.

haciéndoles partícipes de ella, y propiciando un escrutinio más intenso de la actividad pública.

No obstante, la transparencia cumple otra finalidad de primer orden: servir de cauce de profundización en la dimensión democrática del Estado mejorando la posibilidad de participación de los ciudadanos en los asuntos públicos, e implementar la dimensión democrática del Estado sobre la base de una ciudadanía mejor informada.

El profesor LAGUNA DE PAZ expone que la relación entre el poder público y los ciudadanos se manifiesta, en buena medida, en la generación de un importante flujo informativo que opera en un doble sentido: de los ciudadanos hacia los poderes públicos y de los poderes públicos a los ciudadanos. Respecto del primer sentido del flujo informativo, es decir, el que tiene su origen en los ciudadanos que suministran información a los poderes públicos, y en particular a la Administración, se constata que estos últimos, en el ejercicio de sus funciones manejan un importante volumen de información que se integra, no solo por la que ellos mismos producen, sino también por la que recaban de los ciudadanos, bajo el amparo del principio de legalidad (en el curso de los procedimientos administrativos, imposición de deberes de identificación, comunicación, *etc.*) y que encuentra su justificación en la necesidad de atender debidamente al cumplimiento de la diversidad de funciones que tienen encomendadas. En el segundo sentido apuntado, el que tiene como destinatarios a los ciudadanos, la transparencia de los poderes públicos hace referencia a su visibilidad, y no solo afecta a su funcionamiento o forma de proceder sino también, en su forma más plena, alcanza a buena parte de los contenidos que produce lo cuales, a su vez, usualmente incorporan parte de la información recabada de los ciudadanos.

De esta forma, el flujo informativo opera no solo en el doble sentido indicado (Administración-ciudadanos directamente interesados), sino también en una doble dirección que conecta a la Administración (en general a los poderes públicos) no solo con los ciudadanos directamente concernidos, sino también con terceros no directamente afectados pero que participan del interés público de la información cuya obtención se instrumenta, bien a

través de la publicidad que ofrece directamente la Administración, o bien mediante la respuesta a su demanda informativa[467].

No se puede pasar por alto que los avances técnicos con los que contamos en la actualidad han venido a incidir de manera directa en esta cuestión, produciendo un efecto paradójico. De un lado, sin duda los nuevos medios han contribuido de manera decisiva a que los ciudadanos seamos «más visibles» para la Administración, no solo por el volumen de información que le permiten recabar en uso de sus potestades, sino también por las posibilidades de acumulación y tratamiento informativo.

Pero los actuales medios técnicos influyen también en la otra dirección apuntada, incrementando notablemente las posibilidades de eficacia de la transparencia o el flujo informativo desde los poderes públicos a los ciudadanos, sobre todo por la accesibilidad que aquéllos comportan.

En definitiva, la técnica viene a hacer posible la acumulación y completitud de la información, pero su utilización también permite su visibilidad absoluta, y una publicidad absoluta es un camino de no retorno que se compadece mal tanto con el cumplimiento de algunas de las funciones administrativas, de forma excepcional, como también con la preservación de un ámbito de libertad de los ciudadanos, de la Administración, por un lado, y del público en general.

Así, aun cuando la plenitud del principio de transparencia debiera venir de la mano del reconocimiento a los ciudadanos de un amplio derecho de acceso a la información pública que actúe verdaderamente como regla general, la búsqueda del necesario equilibrio entre los diversos derechos e intereses concurrentes impide que la transparencia sea total y absoluta.

Ello nos remite a la tarea de encontrar puntos de encuentro y equilibrio que eviten el sacrificio absoluto de un interés u otro. De un lado, el derecho a la intimidad (en sentido amplio) tanto de los ciudadanos como de los servidores

---

[467] Laguna De Paz, J. C. (2010). Principio de confidencialidad. En Santamaría Pastor, J. A. (Dir.). *Los principios jurídicos del Derecho Administrativo.* Madrid: La Ley p. 1212

públicos. De otro, la propia eficacia de la función administrativa o, en general, de la función pública que se desempeñe; los intereses colectivos básicos como la seguridad, el orden o la propia existencia del Estado y, en todos los casos, las exigencias de la formación de una opinión pública libre y, en definitiva, el derecho de participación de los ciudadanos en los asuntos públicos, son intereses llamados a enfrentarse.

La conjugación de estos intereses diversos se manifiesta en el establecimiento de límites de confidencialidad al flujo informativo en el doble sentido apuntado: de los ciudadanos a los poderes públicos, y de estos a los ciudadanos.

3.6.2 Excepciones del Reglamento (CE) 1049/2001

Afirma MORETÓN TOQUERO[468] que los modelos para definir tales límites o excepciones son diversos. Lo más usual venía siendo indicar excepciones absolutas y relativas, en función de que el acceso no fuese posible o dependiese de la ponderación de diversos intereses o valores jurídicos, y en especial el interés público en revelar o no la información. En este sentido quizá tenga interés hacer una referencia a la regulación de las excepciones del artículo 4 del Reglamento (CE) 1049/2001, ya sean absolutas o relativas, y a los principios generales que sobre el alcance de tales excepciones o límites cabe extraer.

El Considerando 11 de éste, recoge expresamente que: «en principio, todos los documentos de las instituciones deben ser accesibles al público. No obstante, deben ser protegidos determinados intereses públicos y privados a través de excepciones… Al evaluar las excepciones, las instituciones deben tener en cuenta los principios vigentes en la legislación comunitaria relativos a la protección de los datos personales, en todos los ámbitos de actividad de la Unión».

---

[468] Moretón Toquero, A. (2014). Los límites del derecho de acceso a la información pública. *Revista jurídica de Castilla y León, 33*. En http://www.jcyl.es/web/jcyl/binarios/456/748/5.-%20Arancha%20Moret%C3%B3n%20digital.pdf.

Conforme se declara en el apartado primero del artículo 4 a la hora de regular las excepciones absolutas, las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de: a) el interés público por lo que respecta a: i) la seguridad pública; ii) la defensa y los asuntos militares; iii) las relaciones internacionales; o iv) la política financiera, monetaria o económica de la Comunidad o de un Estado miembro; b) la intimidad y la integridad de las personas, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales.

Por su parte, el número 2 del mismo artículo 4 recoge las excepciones relativas. Señala que las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de: i) los intereses comerciales de una persona física o jurídica, incluidos la propiedad intelectual; ii) los procedimientos judiciales y el asesoramiento jurídico; o iii) el objetivo de las actividades de inspección, investigación y auditoría, «salvo que su divulgación revista un interés público superior». Es decir, debe llevarse a cabo una ponderación del perjuicio que pueda suponer el acceso y el interés público que pueda justificar dicho acceso.

El Tribunal de Primera Instancia (Sala Cuarta), en la Sentencia de 7 de febrero de 2002, Aldo Kuijer contra Consejo, asunto T-211/00[469], afirma en su apartado 55 que «el acceso del público a los documentos de las instituciones constituye el principio jurídico y la posibilidad de denegación es la excepción. Una decisión de denegación solo es válida si se basa en una de las excepciones previstas en el artículo 4 de la Decisión 93/731. Conforme a jurisprudencia reiterada, dichas excepciones deben interpretarse y aplicarse restrictivamente, de modo que no se frustre la aplicación del principio general consagrado en dicha Decisión [véanse la sentencia del Tribunal de Primera Instancia de 17 de junio de 1998, Svenska Journalistförbundet/Consejo, T-174/95. Rec. P. II-2289, apartado 110, y para

[469] El texto completo de la Sentencia puede consultarse en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62000TJ0211&from=ES

las disposiciones correspondientes de la Decisión 94/90/CECA, CE, Euratom de la Comisión, de 8 de febrero de 1994, sobre el acceso del público a los documentos de la Comisión (DO L 46, p.58), la sentencia del Tribunal de Primera Instancia de 5 de marzo de 1997, WWF UK/Comisión, T-105/95, Rec. p. II-313, apartado 56]».

En idéntico sentido se pronuncian, por un lado, la Sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager contra Comisión, asunto T-194/04[470], al declarar expresamente en su apartado 107 in fine que el objetivo del Reglamento número 1049/2001 es garantizar, de la manera más completa posible, el derecho de acceso del público a los documentos en poder de las instituciones, y por otro, la Sentencia del Tribunal de Justicia (Gran Sala), de 29 de junio de 2010, Comisión contra Bavarian Lager, asunto C-28/08 P[471], al afirmar explícitamente en su apartado 55 que «el Reglamento número 1049/2001 establece como regla general el acceso del público a los documentos de las instituciones, pero prevé excepciones por razón de determinados intereses públicos y privados. En particular, el undécimo considerando de ese Reglamento recuerda que, «al evaluar las excepciones, las instituciones deben tener en cuenta los principios vigentes en la legislación comunitaria relativos a la protección de los datos personales, en todos los ámbitos de actividad de la Unión».

Tal y como se expone en la Sentencia del Tribunal de Primera Instancia (Sala Cuarta) de 14 de octubre de 1999, Bavarian Lager contra Comisión, asunto T-309/97[472], en la que en su apartado 39 en Tribunal afirma que «procede recordar que las excepciones en el acceso a los documentos deben interpretarse y aplicarse restrictivamente, de modo que no se frustre

---

[470] El texto completo de la Sentencia puede consultarse en http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:62004TJ0194&from=ES

[471] El texto completo de la Sentencia puede consultarse en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62008CJ0028&from=ES

[472] El texto completo de la Sentencia puede consultarse en http://curia.europa.eu/juris/showPdf.jsf?text=&docid=44788&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=116009

la aplicación del principio general consistente en otorgar al público «el máximo acceso posible a los documentos que obran en poder de la Comisión» (sentencias WWF, § 56, Van der Wal, § 41, e Interporc/Comisión, § 49)». En idéntico sentido se pronuncia la Sentencia del Tribunal de Primera Instancia (Sala Quinta) de 23 de noviembre de 2004, Maurizio Turco contra Consejo, asunto T-84/03[473], estas excepciones deben interpretarse y aplicarse de manera estricta, con el fin de que no se frustre el principio general de acceso. Así, en el apartado 60, el Tribunal declara que «las excepciones al acceso a los documentos deben interpretarse y aplicarse restrictivamente, de modo que no frustre la aplicación del principio general consistente en otorgar al público el máximo acceso posible a los documentos que obran en poder de las instituciones».

Las excepciones deben interpretarse teniendo en cuanta el principio del derecho a la información y del principio de proporcionalidad. Así se desprende de la Sentencia del Tribunal de Primera Instancia (Sala Cuarta), en la Sentencia de 7 de febrero de 2002, Aldo Kuijer contra Consejo, asunto T-211/00[474], al afirma en su apartado 57 «la interpretación del artículo 4, apartado 1, de la Decisión 93/731 debe efectuarse a la luz del principio del derecho a la información y del principio de proporcionalidad. De ello se desprende que el Consejo está obligado a examinar su procede conceder un acceso parcial, limitado a los datos no amparados por las excepciones. Con carácter extraordinario, podría admitirse una excepción a dicha obligación de conceder un acceso parcial cuando la carga administrativa provocada por la disimulación de los datos no comunicables se revelara extremadamente gravosa, excediendo así de los límites de lo que puede exigirse razonablemente».

---

[473] El texto completo de la Sentencia puede consultarse en http://curia.europa.eu/juris/showPdf.jsf?text=&docid=49702&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=115108

[474] El texto completo de la Sentencia puede consultarse en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:62000TJ0211&from=ES

Sin embargo, el 30 de abril del año 2008 la Comisión presentó una propuesta de Reglamento del Parlamento Europeo y del consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión[475].

Bajo nuestro criterio, las medidas más interesantes en ésta son las relacionadas con la actualización de los puntos referentes a la definición de documento, la relación existente entre el Reglamento número 1049/2001 y el Reglamento número 45/2001[476], y el régimen de excepciones al acceso a los documentos.

Así, toda persona física o jurídica tendrá derecho a acceder a los documentos de las instituciones. Por "documento" entendemos «todo contenido, sea cual fuere su soporte (escrito en versión papel o almacenado en forma electrónica, grabación sonora, visual o audiovisual) elaborado por una institución y transmitido formalmente a uno o más destinatarios, o bien registrado o recibido de otro modo por una institución; los datos contenidos en sistemas de almacenamiento, tratamiento y recuperación electrónica son documentos si pueden extraerse en forma de listado o formato electrónico utilizando las herramientas disponibles para la explotación del sistema»[477].

---

[475] Comisión de las Comunidades Europeas. (2008). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión. COM(2008) 229 final, , de 30 de abril de 2008. El texto completo de la propuesta se encuentra accesible en http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2008:0229:FIN:EN:PDF

[476] Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos (DO L 8 de 12.1.2001)

[477] A su vez, el 29 de noviembre de 2011 el Parlamento ha emitido el I Informe sobre sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (versión refundida) (COM(2008)0229 – C7-0184/2008 – 2008/0090(COD)). El texto se encuentra accesible en http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2011-0426+0+DOC+PDF+V0//ES. En relación al término "documento", ha propuesto ampliar la definición de la Comisión. De esta manera, se entenderá por «documento», todo contenido, sea cual fuere su soporte (escrito en versión papel o almacenado en forma electrónica, grabación sonora, visual o audiovisual) referente a asuntos relativos a las políticas, acciones y decisiones que entran en el

El punto de partida del Reglamento es el acceso a los documentos, y no el acceso a la información como tal. Por tanto, el soporte del documento no es decisivo. Ahora bien, tal como afirmó el Tribunal de Primera Instancia en la Sentencia de 25 de abril de 2007, WWF European Policy Programme contra Consejo, asunto T-264/04[478], «sería contrario al imperativo de transparencia del que resulta el Reglamento número 1049/2001 que las instituciones se prevalezcan de la inexistencia de documentos para eludir la aplicación de dicho Reglamento. El ejercicio efectivo del derecho de acceso a los documentos presupone que las instituciones afectadas procedan, en la medida de lo posible y de forma no arbitraria y previsible, a la elaboración y conservación de la documentación relacionada con su actividad». Así pues, en opinión del Tribunal, las instituciones implicadas deberán, en la medida de lo posible y de manera no arbitraria y previsible, redactar y mantener documentación relativa a sus actividades. En caso contrario, no podrá ejercerse efectivamente el derecho de acceso a los documentos[479].

En relación al régimen de excepciones, destacamos el nuevo apartado quinto que se añade, por parte de la Comisión, al artículo 4 del Reglamento número 1049/2001 por el que «se divulgarán los nombres, cargos y

---

ámbito de la responsabilidad de una institución, un órgano o un organismo de la Unión. Los datos contenidos en sistemas de almacenamiento, tratamiento y recuperación electrónica, incluidos los sistemas externos utilizados para el trabajo de la institución, constituyen un documento, en particular si pueden extraerse utilizando cualquier herramienta razonablemente disponible para la explotación del sistema en cuestión. Una institución, un órgano o un organismo que quiera crear un nuevo sistema de almacenamiento electrónico, o modificar sustancialmente un sistema existente, deberá evaluar el impacto probable sobre el derecho de acceso, velar por que se garantice el derecho de acceso como derecho fundamental, y actuar a fin de promover el objetivo de transparencia. Las funciones para la recuperación de la información almacenada en sistemas de almacenamiento electrónico deberán adaptarse para satisfacer las solicitudes del público».

[478] El texto completo de la Sentencia puede consultarse en el siguiente link:

http://curia.europa.eu/juris/showPdf.jsf?text=&docid=61308&pageIndex=0&doclang=ES&mode=lst&dir=&occ=first&part=1&cid=210552

[479] Véase el Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DOUE 2009/C 07/01/2009). El texto se encuentra accesible en https://edps.europa.eu/sites/edp/files/publication/08-06-30_access_documents_es.pdf

funciones de los titulares de cargos públicos, funcionarios y representantes de intereses relacionados con la actividad profesional salvo que, por circunstancias particulares, tal divulgación pueda perjudicar a las personas afectadas. Se divulgarán otros datos personales de conformidad con las condiciones de tratamiento legal de tales datos establecidas en la legislación de la CE en materia de protección de las personas en lo que respecta al tratamiento de datos personales».

Por su parte, el Parlamento Europeo en el I Informe sobre sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (versión refundida) (COM(2008)0229 – C7-0184/2008 – 2008/0090(COD)) ha venido a acotar y a especificar la propuesta presentada por la Comisión Europea. Así, a la hora de ponderar la existencia de un posible perjuicio, se diferencia si los datos se refieren exclusivamente a actividades profesionales, si se trata de una persona pública o privada, y si han sido publicados con el consentimiento del afectado con antelación. Del mismo modo, en la ponderación se tendrá en cuenta la posible existencia de un interés público superior en su divulgación. El texto propuesto por el Parlamento queda redactado así:

> *«5. Los datos personales no se divulgarán si la divulgación perjudica la intimidad o la integridad de la persona en cuestión. No se considerará que se ha causado ese perjuicio: i) si los datos se refieren exclusivamente a la actividad profesional de la persona afectada salvo que, por circunstancias particulares, haya motivos para suponer que tal divulgación pueda perjudicar a dicha persona; ii) si los datos se refieren exclusivamente a una persona pública, salvo que, por circunstancias particulares, haya motivos para suponer que tal divulgación pueda perjudicar a dicha persona o a otras personas relacionadas con ella; iii) si los datos ya han sido publicados con el consentimiento de la persona afectada. No obstante, se divulgarán los datos personales si un interés público superior exige su divulgación. En tal caso, la institución, el órgano o el organismo en cuestión estará obligado a especificar el interés*

público. Deberá asimismo explicar las razones por las que, en ese caso concreto, el interés público prevalece sobre el interés de la persona afectada. Cuando una institución, un órgano o un organismo deniegue el acceso a un documento sobre la base del presente apartado, deberá considerar si es posible dar un acceso parcial a dicho documento».

Por su parte, el artículo 3 del Convenio 205 del Consejo de Europa sobre el Acceso a los Documentos Públicos, firmado 18 de septiembre de 2009, establece los posibles límites al acceso a los documentos públicos[480]. Este Convenio opta por un modelo en el que no se hace distinción alguna entre excepciones relativas o absolutas, y tipifica un total de once supuestos cuya concurrencia permite limitar el acceso. Este es el sistema seguido por nuestro legislador nacional al especificar los límites al derecho de acceso en el artículo 14[481] de la LTBG.

---

[480] «Artículo 3 – Posibles límites al acceso a los documentos públicos 1) Cada Parte puede limitar el derecho del acceso a los documentos públicos. Los límites deberán estar previstos por una ley, ser necesarios en una sociedad democrática y tener como objetivo la protección de: a) la seguridad nacional, la defensa y las relaciones internacionales; b) la seguridad pública; c) la prevención, la investigación y el procesamiento de actividades criminales; d) las investigaciones disciplinarias; e) la inspección, control y supervisión por autoridades públicas; f) la intimidad y otros intereses privados legítimos; g) los intereses económicos y comerciales; h)las políticas estatales de cambio de moneda, monetarias y económicas; i) la igualdad de las partes en los procedimientos judiciales y la administración eficaz de la justicia; j) el medio ambiente; o k) las deliberaciones dentro o entre autoridades públicas en lo referente al examen de un asunto. Los Estados interesados, a la hora de la firma o al depositar su instrumento de ratificación, aceptación, aprobación o adhesión, mediante una declaración enviada al Secretario General del Consejo de Europa, pueden declarar que las comunicaciones oficiales con la Familia Real y su Casa Real o el Jefe de Estado también están incluidas entre las posibles limitaciones. 2) El acceso a la información contenida en un documento oficial puede ser rechazado si puede o probablemente pueda dañar los intereses mencionados en el párrafo 1, a menos que haya un interés público que prevalezca en dicha revelación. 3) Las Partes considerarán la posibilidad de fijar unos plazos más allá de los cuales los límites mencionados en el párrafo 1 dejen de ser aplicables».

[481] «Artículo 14. Límites al derecho de acceso. 1. El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para: a) La seguridad nacional. b) La defensa. c) Las relaciones exteriores. d) La seguridad pública. e) La prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios. f) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva. g) Las funciones administrativas de vigilancia, inspección y control. h) Los intereses económicos y comerciales. i) La política económica y monetaria. j) El secreto profesional y

El profesor PIÑAR MAÑAS afirma que esta norma responde a los estándares normales de acceso a la información, siempre que se apliquen escrupulosamente los criterios de la jurisprudencia del Tribunal de Justicia, y sobre todo, siempre que no se abuse del silencio negativo. Si bien es usual en el panorama comparado que la falta de resolución ante la petición inicial de acceso permita considerar desestimada la petición (como ocurre en nuestro caso según el artículo 20.4[482] de la Ley), no ocurre lo mismo en relación con la falta de resolución de la reclamación interpuesta ante el órgano de tutela, que suele dar pie a entender estimada la impugnación[483]. La ley también ha diseñado un mecanismo de silencio negativo ante la falta de resolución expresa tras presentar la impugnación ante el Consejo de Transparencia[484], de modo que podemos encontrarnos ante un doble silencio negativo. Pues bien, un hipotético y no deseable uso excesivo del silencio puede dar al traste literalmente con el derecho de acceso, pues se hurtaría a los interesados no solo su derecho a acceder a la información pública, sino a que se les hagan saber los motivos por los que en su caso el acceso puede ser denegado.

---

la propiedad intelectual e industrial. k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión. l) La protección del medio ambiente. 2. La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso. 3. Las resoluciones que de conformidad con lo previsto en la sección 2.ª se dicten en aplicación de este artículo serán objeto de publicidad previa disociación de los datos de carácter personal que contuvieran y sin perjuicio de lo dispuesto en el apartado 3 del artículo 20, una vez hayan sido notificadas a los interesados».

[482] «Artículo 20. Resolución. 4. Transcurrido el plazo máximo para resolver sin que se haya dictado y notificado resolución expresa se entenderá que la solicitud ha sido desestimada».

[483] Piñar Mañas, J. L. (2014). Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno. *Revista catalana de dret públic, 49, p. 13*. En http://revistes.eapc.gencat.cat/index.php/rcdp/article/download/10.2436-20.8030.01.29/n49-pinar-es.pdf

[484] «Artículo 24. Reclamación ante el Consejo de Transparencia y Buen Gobierno. 4. El plazo máximo para resolver y notificar la resolución será de tres meses, transcurrido el cual, la reclamación se entenderá desestimada».

3.6.3 Los límites del derecho de acceso en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno

En todos los sistemas jurídicos, sean supranacionales o nacionales, se contemplan límites al derecho de acceso a la información. No existe ninguno de ellos en el que toda información, cualquiera que sea la materia y los posibles efectos de su divulgación. pueda ser objeto de divulgación.

Los límites al derecho de acceso deben ser tasados, mediante un sistema de lista exhaustiva, cerrada, referidos a la necesidad de tutela de bienes públicos o privados o concurrentes. (como regla general, no deben aplicarse en bloque por materias (esto es, no toda información sobre una determinada materia debe estar vedada al conocimiento público), sino entrando a conocer si la información solicitada puede provocar un perjuicio efectivo a un bien o derecho de los contemplados en la lista que justifica una limitación al derecho de acceso (es el llamado «test del perjuicio o del daño», que en algunos Derechos, además, se exige que revista, en ciertos supuestos, una especial gravedad).

Además, una vez constatado que la divulgación de la información supondría un perjuicio para uno de los bienes enunciados en las leyes como justificativos de una limitación al acceso, en algunos sistemas jurídicos procede la denegación de información (en el caso de la publicidad pasiva) o su no publicación (en el caso de la publicidad activa).

Cuando hay un afectado (porque se trata de información elaborada o relativa a un tercero, sea un sujeto público o privado) muchos sistemas exigen que se le consulte y le otorgan o bien un derecho de veto o bien. más Ilimitadamente, exigen que se tome en cuenta su argumentación.

Además, todos ellos buscan maximizar el derecho de acceso, de forma que contemplan la posibilidad de dar un acceso parcial (y/o anonimizado, en el caso de que la información contenga datos personales) y restringen la vigencia de las limitaciones en el tiempo. bien en un plazo fijo o bien hasta el momento en que dejan de estar justificadas. o mediante una combinación de ambas técnicas.

En cuanto a cuáles sean dichos límites, puede decirse que se trata de intereses públicos (la defensa. las relaciones internacionales, la seguridad exterior e interior y la lucha contra el crimen. la economía y las finanzas públicas; la protección del medio ambiente; la tutela judicial y el correcto funcionamiento de la justicia; la efectividad de las actividades públicas de vigilancia y control; la existencia de un espacio libre de presiones e influencias en el proceso de toma de decisiones públicas) y privados (la vida privada, en especial en lo tocante a la salud y la seguridad de las personas; los intereses comerciales y económicos, incluidas la propiedad intelectual e industrial).

En particular, en cuanto a las relaciones entre publicidad y privacidad, puede decirse que en el potencial conflicto entre publicidad y privacidad de la información administrativa, prevalece la reserva de los datos íntimos, que vienen a identificarse en buena medida con los que la normativa sobre protección de datos califica como «especialmente protegidos» o «sensibles» (relativos a la ideología, creencia, religión, raza, vida sexual, salud, a los que se une un régimen también diferenciado de los datos sobre condenas penales o administrativas), y cuyo conocimiento es susceptible de ocasionar un perjuicio grave a los afectados.

La categoría de los datos especialmente protegidos supone una importante directriz para dilucidar cuándo una publicidad inconsentida por la vía del otorgamiento del acceso puede implicar una mayor injerencia en los derechos constitucionales de los afectados, y, por ende, debe ser excepcional, solo justificada por la prevalencia de otro derecho fundamental. A ellos solo puede accederse cuando una ley ponderadamente así lo prevea para la salvaguarda de otros bienes superiores, como de hecho prevén las propias normas sobre protección de datos respecto de los datos de salud cuyo conocimiento sea necesario para dar respuesta a una urgencia vital para la vida y la integridad de las personas.

Fuera de los casos de previsión legal, resulta razonable que solo puede accederse a los datos íntimos por vía de requerimiento judicial en el seno de un proceso, como ocurre con las manifestaciones «espaciales» de la intimidad como el domicilio o las comunicaciones. Estando en juego el

derecho a la intimidad, tiene sentido su tratamiento como una excepción imperativa, de modo que no dependa de la apreciación discrecional de la autoridad administrativa. Por el contrario, debe prevalecer la publicidad de los datos personales que, sin ser íntimos, están directamente relacionada con la organización, la gestión y el gasto públicos, esto es, cuando se trata de acceder a información relevante para conocer la corrección de la actuación administrativa relativa no a la vida privada de las personas sino a la relación entre el poder público y sus propios empleados, contratistas, agentes, beneficiarios de subvenciones, permisos, etc.

Mayoritariamente, son las leyes de acceso las que regulan estos principios, si bien en algunos casos, minoritarios, remiten la regulación a las leyes sobre protección de datos.

En lo que hace a las relaciones entre publicidad y secretos oficiales, las leyes de acceso suelen contemplar entre sus límites la defensa, las relaciones internacionales, la seguridad nacional, la seguridad pública o la persecución de los delitos. La regulación de los secretos oficiales suele quedar regulada al margen de las leyes de acceso. sin que haya un único parámetro de engarce entre ambas normativas, siendo las opciones más comunes o bien excluir la información clasificada del ámbito de aplicación de las leyes de acceso y remitir a lo que dispongan dichas regulaciones las posibilidades de acceso a esa información, o bien guardar silencio sobre el particular.

3.6.3.1 Los límites del artículo 14 LTBG

La LTBG ha optado por establecer un listado de bienes cuya posible afectación en caso de concederse cl acceso puede limitar el derecho en su artículo 14. Son los siguientes:

> *«a) La seguridad nacional. b) La defensa. c) Las relaciones exteriores. d) La seguridad pública. e) La prevención, investigación y sanción de los ilícitos penales. administrativos o disciplinarios. j) La igualdad de las partes en los procesos judiciales y la tutela judicial efectiva. g) Las funciones administrativas de vigilancia. inspección y*

control. h) Los intereses económicos y comerciales i) La política económica y monetaria. j) El secreto profesional y la propiedad intelectual c industrial. k) La garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión. l) La protección del medio ambiente».

Por su parte, el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos[485] (CEADP) establece los posibles límites al acceso a los documentos públicos en los siguientes términos:

«1) Cada Parte puede limitar el derecho del acceso a los documentos públicos. Los límites deberán estar previstos por una ley, ser necesarios en una sociedad democrática y tener como objetivo la protección de: a) la seguridad nacional, la defensa y las relaciones internacionales; b) la seguridad pública; c) la prevención, la investigación y el procesamiento de actividades criminales; d) las investigaciones disciplinarias; e) la inspección, control y supervisión por autoridades públicas; f) la intimidad y otros intereses privados legítimos; g) los intereses económicos y comerciales; h)las políticas estatales de cambio de moneda, monetarias y económicas; i) la igualdad de las partes en los procedimientos judiciales y la administración eficaz de la justicia; j) el medio ambiente; o k) las deliberaciones dentro o entre autoridades públicas en lo referente al examen de un asunto.»

Si comparamos ambos listados, vemos que apenas hay diferencias significativas[486], siendo la única aparentemente relevante el trueque de la

---

[485] Convenio sobre Acceso a los Documentos Públicos, Tromsø, 18 de junio de 2009.

[486] Las diferencias son la alusión a las relaciones «exteriores» y no «internacionales» (muy en especial para dar cuenta del fenómeno comunitario). la alusión a la «tutela judicial efectiva» en lugar de «la eficacia de la Administración de justicia» (para adecuar la referencia al marco constitucional). y a «la garantía de la confidencialidad o el secreto requerido en procesos de toma de decisión», al que el CEADP alude como «las deliberaciones dentro o entre autoridades públicas en lo referente al examen de un asunto».

noción de «otros intereses privados legítimos», utilizada en el CEADP, por la de «el secreto profesional y la propiedad intelectual e industrial».

3.6.3.1.1 El punto de partida: la información pública y el «interés público»

El objeto del derecho de acceso es la «información pública»[487] y de conformidad con lo previsto en el artículo 13 LTBG, *«se entiende por información pública los contenidos o documentos, cualquiera que sea su forma-to o soporte, que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones»*.

Por lo tanto, una interpretación conforme con el principio de accesibilidad máxima, acorde con una configuración amplia del derecho de acceso (a la que se refiere la Exposición de Motivos) requiere que la posibilidad de acceso sea efectivamente la regla general, permitiendo que el ejercicio de este derecho recaiga sobre todas las informaciones de las que disponen los poderes públicos, en la línea de lo que señala el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos, cuando en su Preámbulo manifiesta que «todos los documentos públicos son en principio públicos y solamente pueden ser retenidos para proteger otros derechos e intereses legítimos», y remarcando también con ello el carácter instrumental de la publicidad.

En este sentido, el derecho a recibir información [artículo 20.1.d) CE] como «derecho a informarse» (y no como mera vertiente pasiva del derecho a informar) que integra la facultad de acudir a las fuentes informativas (en este caso la Administración o los poderes públicos son la fuente), se encuentra en la base del derecho de acceso. Este fundamento, a su vez, aporta una dimensión objetiva o institucional por cuanto la libertad de información fomenta el libre flujo informativo, que es presupuesto necesario de la

[487] El artículo 12 LTBG declara expresamente que «todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley. Asimismo, y en el ámbito de sus respectivas competencias, será de aplicación la correspondiente normativa autonómica».

participación de los ciudadanos en los asuntos públicos, tal y como recoge el artículo 23.1 CE[488]. Una «participación informada» exigencia del principio democrático y a la vez actúa como contrapoder, contribuyendo a disuadir de las conductas inapropiadas y, en último término, a disminuir la corrupción.

No obstante, este planteamiento general, cuando la LTBG se refiere a la aplicación de los límites en su artículo 14.2 señala que «la aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso». Esta referencia al interés privado superior al que protegen los límites previstos legalmente, y que puede fundamentar el acceso, ha sido interpretado negativamente por la doctrina[489].

3.6.3.1.2 La previsión legal sobre los límites al derecho de acceso

La Exposición de Motivos de la LTBG señala las líneas básicas del complejo sistema de límites del derecho de acceso que posteriormente desarrolla, de manera principal, en los arts. 14 y 15. Los aspectos básicos del sistema de límites que establece la LTBG se pueden sintetizar en los siguientes aspectos:

En, primer lugar, el sistema que sigue la Ley es el de la previsión de un listado único de límites que recoge a las materias (artículo 14 LTBG) que eventualmente pueden entrar en conflicto con el derecho de acceso,

---

[488] «Los ciudadanos tienen el derecho a participar en los asuntos públicos, directamente o por medio de representantes, libremente elegidos en elecciones periódicas por sufragio universal».

[489] Acerca de la previsión legal de concurrencia de un interés público o «privado» del solicitante, Emilio GUICHOT señala con acierto que «el derecho de acceso no es un derecho instrumental al servicio de la protección de otros derechos, sino un derecho autónomo al servicio de la transparencia, la participación y el control de la actuación pública, conectado con el Estado democrático y, por ende, al margen de cualquier distinción en función de la motivación que pueda tener el solicitante. Dicho de otro modo, el único parámetro con el que confrontar la protección de los límites es el valor que para la sociedad tiene el cono-cimiento de la información, un juicio abstracto desvinculado por completo de la cualidad y motivación del solicitante». *Vid.* Guichot Reina, E. (2014). *Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, de 9 de diciembre*. Madrid: Tecnos, pp. 118 y 119.

asumiendo el criterio adoptado por el Consejo de Europa en el Convenio sobre Acceso a los Documentos Públicos.

En segundo lugar, para apreciar el conflicto que puede justificar la limitación del derecho de acceso, la norma remite a la aplicación previa de «un test de daño» (harm test), es decir, a la comprobación del perjuicio que el acceso a determinada información pueda producir sobre el interés que se pretende salvaguardar con la confidencialidad.

Por tanto, en ningún caso parece que quepa una limitación absoluta, sino que, por el contrario, será preciso constatar el eventual daño que la publicidad pue-de causar a los intereses protegidos por dichas materias.

Hay que observar que, siguiendo un principio pro acceso, la Ley exige un daño y no un mero peligro para los otros bienes concurrentes que intenta proteger. Esto requiere, por tanto, que la decisión denegatoria del acceso sea suficiente motivada (como exige el artículo 20.2 LTBG), a fin de que la procedencia de dicha denegación pueda ser controlada en vía de recurso.

Advertido el potencial daño que pudiera ocasionarse con el acceso a la información solicitada, la resolución del conflicto se llevará a cabo mediante un ejercicio de ponderación (*balancing test*) en el que, se tendrán en cuenta, por un lado, el interés público en la divulgación de la información y, por otro, los derechos e intereses protegidos por la lista de materias indicada, para decidir cuál deba ser finalmente objeto de protección o, en su caso, como solución intermedia, optar por reconocer un acceso parcial como vía para conciliar ambos intereses (artículo 16 LTBG). Efectivamente, en los casos en los que la aplicación de los límites del artículo 14 LTBG no afecte a la totalidad de la información, la Ley indica que se concederá el acceso parcial, lo que consistirá en facilitar la información, pero omitiendo aquella parte que se encuentre afectada por el límite.

Ahora bien, este acceso parcial tiene a su vez su límite en la conservación del propio sentido de la información proporcionada, con lo que quedará excluido el acceso parcial cuando de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante qué parte de la información ha sido omitida.

La cuestión es quién ha de valorar si con el acceso parcial se produce, o no, la distorsión informativa. Solo quien tiene la información puede hacer una valoración cabal acerca de este extremo. Por tanto, la pretensión del ciudadano, privado de esta facultad de valoración, queda a merced de la decisión del órgano obligado a suministrar la información y sin posibilidad de control.

Por tanto, aunque la posibilidad de acceso parcial favorece prima facie el ejercicio de este derecho de acceso manteniendo los límites en un campo de acción estricto, este beneficio en la práctica solo es aparente, pues la intensidad de la afectación o la apreciación del grado de distorsión o no de la información, o su pérdida de sentido, son valoraciones que quedan en manos del responsable de suministrarla.

Sin embargo, tratándose de un acceso parcial, parece que esta técnica, unida a las posibilidades de disociación de datos, puede lograr el fin informativo previsto en los casos en los que los límites no afectan a toda la información; es decir, que los límites al suministro parcial de información deben también ser aplicados restrictivamente.

En íntima conexión con los límites al derecho de acceso, resulta oportuno referirse a las previsiones del artículo 18 de la Ley respecto de las causas que pueden motivar la denegación de plano de la solicitud de acceso a la información. En este precepto, donde se regula el procedimiento de ejercicio de este derecho, se excluye el acceso a la información, con carácter imperativo, en los cinco supuestos que el precepto enuncia:

> *«i) Que se refieran a información que esté en curso de elaboración o de publicación general; ii) Referidas a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas; iii) Relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración; iv) Dirigidas a un órgano en cuyo poder no obre la información cuando se desconozca el competente; v) Que sean manifiestamente*

repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta Ley».

3.6.3.1.3 Las materias que puedan limitar el derecho de acceso

Ya hemos visto que el artículo 14 de la LTBG relaciona una docena de materias que pueden limitar el acceso a la información, y destina el precepto siguiente a tratar de forma separada el eventual conflicto que se pudiera plantear entre el derecho de acceso y el derecho a la protección de datos personales[490]. Para este último supuesto la ley establece mecanismos de equilibrio específicos tendentes a hacer compatibles ambos derechos aunque el punto de partida es manifiestamente desigual por razón de la diferente naturaleza de los intereses en juego, lo que tiene una evidente repercusión respecto de una eventual ponderación.

Pues bien, al listado del artículo 14 LTBG se ha de añadir la protección de datos personales que, por su naturaleza y especificidad, merece una referencia separada en el artículo 15 LTBG.

De esta forma, cuando la información solicitada (aun no estando comprendida entre las materias enumeradas en el artículo 14 LTBG) pueda afectar de forma directa a la protección de datos personales, entrarán en funcionamiento los mecanismos de equilibrio necesarios establecidos por la Ley.

Como criterio moderador, el artículo 5.3 LTBG infine señala, respecto de la publicidad activa, la necesidad de disociar los datos cuando la información

---

[490] El artículo 105.b) CE enuncia solo tres límites, y su aparente exhaustividad contrasta con el amplio listado previsto por la LTBG. A este respecto señala GUICHOT que «la LRJPAC sentó precedente en 1992, incorporando una cláusula abierta al enunciado de materias que excedían de las aludidas en el citado artículo constitucional, precedente que después siguieron las Leyes de acceso a la información ambiental y de reutilización de la información del sector público, ampliando la enumeración de posibles límites. Y que, en un sistema de valores como es el constitucional, ha de procederse a una interpretación integradora que se resiste a constreñir los posibles bienes en conflicto a los límites acogidos en el artículo 105.b) CE, que no agotan con mucho las posibles colisiones». *Vid.* Guichot Reina, E. (2014). *Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, de 9 de diciembre*. Madrid: Tecnos, p. 109.

que deba darse contuviera datos especialmente protegidos[491]. La disociación, por tanto, es el criterio que se utiliza para equilibrar entre el deber de dar cumplimiento a la obligación informativa y el de protección de los datos personales.

La Ley no hace una descripción negativa del derecho de acceso por oposición a las materias amparadas por el principio de confidencialidad, sino que proclama el derecho de acceso, y a posteriori señala las eventuales circunstancias que pueden limitarlo. No obstante, a mi modo de ver, algunas de estas, en sentido estricto, pueden constituir no meras limitaciones sino verdaderos límites definidores del derecho de acceso, como ocurre con las materias que, bien por decisión de la ley, bien por su propia naturaleza, o bien por declaración de los poderes públicos, se encuentran amparadas por la confidencialidad, en sentido general, o en su manifestación más estricta, por el deber de secreto[492].

Sin perjuicio de lo dicho, hay que remarcar que, a juicio de la doctrina, la previsión legal de los límites es demasiado amplia, al menos desde un punto de vista objetivo, por la indeterminación de su redacción, así como por su eficacia temporal. Respecto de la primera cuestión, resulta llamativa la

---

[491] Artículo 5. Principios generales. «3. Serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos».

[492] El Informe del Consejo de Estado 707/2012, aprobado el 19 de julio de 2012, ya se pronunció sobre este particular en los siguientes términos: «debe señalarse que las materias o ámbitos que se configuran en este artículo como excepciones participan, en puridad, de la naturaleza de auténticos límites al ejercicio del derecho de acceso a la información. Desde esta perspectiva, el Consejo de Estado considera que, en lugar de configurar estos límites como parte integrante de la definición de información pública, acotándola o restringiendo su alcance, sería más correcto técnicamente mencionarlos en un apartado distinto del artículo 9, que podría quedar redactado en unos términos similares a los que a continuación se propone: "No tendrá la consideración de información pública que pueda ser objeto del derecho de acceso regulado en esta Ley aquella cuyo conocimiento perjudique a la seguridad nacional, la defensa, las relaciones exteriores, la seguridad pública o la prevención, investigación y sanción de los ilícitos penales, administrativos o disciplinarios"».

amplitud de la redacción de los límites, así como su ambigüedad[493], cuando precisamente, si convenimos que el hilo conductor de la norma es dar la máxima amplitud al derecho de acceso, esto exige, por el contrario, una interpretación estricta de los límites.

En cualquier caso, conforme al artículo 14.2 LTBG:

> *«La aplicación de los límites será justificada y proporcionada a su objeto y finalidad de protección y atenderá a las circunstancias del caso concreto, especialmente a la concurrencia de un interés público o privado superior que justifique el acceso».*

3.6.3.2 El test del perjuicio, los criterios de ponderación y el acceso parcial

La aplicación de los límites está sometida al test del perjuicio494. Además, conforme al dictado del artículo 14.2 LTBG, ya hemos visto que está sujeta a un principio de maximización del derecho, lo cual implica que las restricciones tengan el mínimo alcance necesario, lo que conecta con el principio de acceso parcial495. Además, permite que incluso en los casos en que el acceso suponga un perjuicio para los bienes en cuestión pueda prevalecer el interés público o privado en conocer la información si éste es juzgado «superior». Aparece aquí como clave de bóveda el principio de ponderación.

---

493 Señala Guichot que el carácter abstracto de la formulación es indiscutible aunque, en su opinión, no cuenta con alternativa razonable, ya que «la realidad es tan proteica que el intento de una definición en positivo resulta un esfuerzo vano abocado al fracaso», *vid.* Guichot Reina, E. (2014). *Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, de 9 de diciembre*. Madrid: Tecnos, p. 109.

494 El apartado primero del artículo 14 LTBG expresamente declara «El derecho de acceso podrá ser limitado cuando acceder a la información suponga un perjuicio para […]»

495 Artículo 16. Acceso parcial. «En los casos en que la aplicación de alguno de los límites previstos en el artículo 14 no afecte a la totalidad de la información, se concederá el acceso parcial previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido. En este caso, deberá indicarse al solicitante que parte de la información ha sido omitida».

La justificación a la que apela el artículo 14.2 LTBG debe entenderse como la llamada a un juicio de apreciación, expresado de forma argumentada, acerca de la efectiva producción de un perjuicio para uno de los bienes protegidos en caso de que la información sea divulgada, activa o pasivamente.

El tema entronca directamente con la motivación exigida por el artículo 20.2 LTBG[496]. Al haber en todos estos casos una limitación a un derecho, es necesario que la limitación tenga como presupuesto efectivo el perjuicio que se provocaría a uno de los bienes públicos o privados mencionados en el apartado primero y que se argumente que el perjuicio realmente se produciría y en qué consistiría. No basta con invocar uno de los bienes relacionados en el elenco del artículo 14.1 LTBG, pues las exclusiones no lo son por materias o por bienes afectados, sino solo en los casos en que dichos bienes puedan ser perjudicados por una divulgación.

Por su parte, como decimos, la proporcionalidad conecta de forma directa con el acceso parcial regulado en el artículo 16. Esta previsión de acceso parcial es absolutamente común en el Derecho supranacional y comparado, y a menudo se lleva a cabo mediante la omisión física de las partes afectadas por la limitación. Más discutible puede resultar la posibilidad excepcional de no conceder acceso alguno en los casos en que la omisión dé lugar a información distorsionada o carente de sentido que, si bien está contemplada en el CEADP, puede dar lugar a abusos en su interpretación por algunos aplicadores, en lugar de que sean los propios destinatarios los que juzguen la utilidad de la información solicitada.

La aplicación de los límites está sometida al principio de ponderación. GUICHOT señala que de la dicción del articulo 14 LTBG podría deducirse que las limitaciones son de apreciación discrecional, expresamente afirma que «el derecho de acceso podrá ser limitado». Sin embargo, prosigue

---

[496] Artículo 20. Resolución. «2. Serán motivadas las resoluciones que denieguen el acceso, las que concedan el acceso parcial o a través de una modalidad distinta a la solicitada y las que permitan el acceso cuando haya habido oposición de un tercero. En este último supuesto, se indicará expresamente al interesado que el acceso sólo tendrá lugar cuando haya transcurrido el plazo del artículo 22.2».

afirmando que resulta difícil pensar que quede a la libre decisión del aplicador el conceder el acceso a una información que perjudique a cualquiera de los bienes mencionados en dicho artículo, unos públicos y otros privados, conectados con derechos fundamentales o intereses de terceros. De este modo, e interpretándolo de conformidad con el propio CEADP, parece que más bien hay que conectar la expresión con la ponderación con el interés público o privado a la que llama el apartado segundo de dicho artículo, a la que hay que proceder en todo caso, incluso si la divulgación puede suponer un perjuicio para los bienes enumerados en el apartado primero, y cuyo resultado «puede» dar lugar a un juicio favorable o «puede» darlo desfavorable al acceso. Por tanto, no se trata de una auténtica discrecionalidad del aplicador, sino de la llamada a un juicio ponderativo caso por caso, y no por materias, cuyo resultado condicionará la decisión sobre acceso.

La posibilidad de que el acceso a una información conlleve un perjuicio, nos sirve para valorar la importancia que para la sociedad pueda tener el conocimiento de la misma, incluso si con el conocimiento de la misma, se causara un hipotético perjuicio.

Sin embargo, la LTBG alude a la posibilidad de que prevalezca un interés público «o privado», frente al del solicitante concreto de información. Afirma GUICHOT que esta previsión, contraria a principios bien asentados en el Derecho supranacional y comparado, supone un grave desconocimiento del fundamento del derecho de acceso, que no es un derecho instrumental al servicio de la protección de otros derechos, sino un derecho autónomo al servicio de la transparencia, la participación y el control de la actuación pública, conectado con el Estado democrático y, por ende, al margen de cualquier distinción en función de la motivación que puede tener el solicitante, que por ello mismo, no exige[497].

Dicho de otro modo, el único parámetro con el que confrontar la protección de los límites es el valor que para la sociedad tiene el conocimiento de la

[497] Guichot Reina, E. Op. cit. pp 118-119

información, un juicio abstracto desvinculado por completo de la cualidad y motivación del solicitante. Lo que, por lo demás, hace que una vez concedido el acceso, la información pueda circular libremente en la sociedad y ser conocida por cualquiera.

La previsión es contradictoria con la falta de exigencia de interés alguno y, por ende, de motivación, con el propio sentido del derecho de acceso y perturba de forma grave el entero sistema y pone en cuestión su acomodación al CEADP y en general al Derecho comparado, en que si hay un principio común es el de excluir la toma en consideración del interés particular del solicitante, dado que se trata de un juicio abstracto de ponderación entre la importancia general para la opinión pública del conocimiento de la información y el perjuicio al bien público o privado confrontado[498].

3.6.4 La protección de datos[499]

En el Derecho supranacional y comparado, la protección de la intimidad, la privacidad o el derecho a la protección de datos, constituyen un límite a la transparencia. En nuestro Ordenamiento Jurídico, la Constitución en su artículo 105.b) alude expresamente a la «intimidad de las personas» como límite.

---

[498] Así, por ejemplo, el Tribunal Supremo de los Estados Unidos, en la sentencia dictada en el asunto *United States Deportment of Justica v. Reporters Committee for Freedom of the Press* [489 United States 749 (1989)], ha sentado el principio según el cual, la apreciación del interés público ha d hacerse en términos objetivos, esto es, en función de la naturaleza de la información y su idoneidad para contribuir a la transparencia y control de la actuación administrativa. Por tanto, el interés personal del solicitante es irrelevante, lo que implica que la Administración debe tratar de igual modo a cualquier solicitante respecto de la misma información, salvo aquella en que el solicitante sea el propio afectado. Es más, ha de hacerse abstracción de la finalidad particular del solicitante, y focalizar en la naturaleza del documento solicitado y su relación con el interés público general, y los posibles efectos de la divulgación en el público en general. Esta perspectiva tiene como consecuencia facilitar un criterio que permite también su aplicación a categorías abstractas de documentos.

[499] En el Capítulo V nos dedicaremos ampliamente a tratar las especificidades del Derecho a la protección de datos como límite a la transparencia. No obstante, no podemos dejar de referirnos a él brevemente en este apartado.

3.6.4.1 La evolución del texto durante la tramitación de la Ley

El primer y segundo Anteproyectos de la LTBG, se hacían eco, de forma sintética, de los principios reconocidos en el Derecho comparado[500]. Se regulaba de forma particularizada la limitación dimanante del derecho a la protección de datos conforme al siguiente esquema. En primer lugar, una determinación de la normativa aplicable, conforme a la cual las solicitudes de información que contengan datos personales de terceros se regirían por la LTBG y solo en el caso de que los únicos datos contenidos sean los del propio solicitante de información sería de aplicación la normativa sobre protección de datos[501]. En el caso de contener datos especialmente protegidos[502], la regla era la denegación del acceso salvo consentimiento expreso y por escrito del afectado. Con carácter general, y salvo concurrencia de circunstancias particulares, prevalecía el derecho a acceso respecto de los datos no íntimos directamente relacionados con la organización, funcionamiento o actividad pública del órgano o, en los demás casos, previa ponderación, si el acceso no perjudicara ningún derecho constitucionalmente protegido. El tratamiento posterior de los datos quedaba sometido a la normativa sobre protección de datos[503].

---

[500] Véase al respecto Guichot Reina, E. (2011). Transparencia y acceso a la información pública en España: análisis y propuestas legislativas. *Fundación Alternativas*, *170, p. 39*. En http://www.fundacionalternativas.org/public/storage/laboratorio_documentos_archivos/a1d04f2c5f4e94e441966c1b79f39fa3.pdf

[501] El artículo 15.1 LOPD expresamente afirma que «el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos».

[502] Categoría de datos recogida en el artículo 7 LOPD, y son los datos referentes a la ideología, religión, creencias, afiliación sindical, origen racial, salud, vida sexual e infracciones penales o administrativas.

[503] Véase el artículo 11 del Anteproyecto de ley de Transparencia, Acceso a la Información Pública y Buen Gobierno, referido a la protección de datos personales. «Artículo 11. Protección de datos personales 1. Cuando la solicitud de acceso se refiera a información pública que contenga datos de carácter personal se aplicarán las disposiciones previstas en esta Ley. No obstante, se aplicará la normativa de protección de datos personales cuando los datos que contenga la información se refieran únicamente al solicitante. 2. Si la información solicitada contuviera datos especialmente protegidos en los términos de la normativa de protección de datos personales, se denegará el acceso salvo que el

Sin embargo, el Informe de la Agencia Española de Protección de Datos[504] marcó por completo la regulación sobre las relaciones entre acceso y privacidad, hasta el punto de que contenía como conclusión una propuesta de redacción alternativa del artículo que sería acogida por el Gobierno, sustituyendo la redacción anterior. Afirma GUICHOT que se trató, a su juicio de un informe y una propuesta con graves defectos de entendimiento de la lógica del derecho de acceso a la información, que fue asumido de forma acrítica por el Gobierno y que introdujo graves distorsiones en la regulación[505].

Ya se ha comentado que se mantuvo en el apartado primero la previsión de que la norma aplicable con carácter general para resolver las solicitudes es la normativa sobre acceso, salvo cuando la información solicitada contenga sólo datos referidos al solicitante, en cuyo caso estará ejerciendo el también llamado «derecho de acceso» de la normativa sobre protección de datos y se aplicará este bloque normativo, si bien se añadió que ello «sin perjuicio de que, en este caso, el otorgamiento del acceso permita el conocimiento por el solicitante no solo de los datos que contenga la información de los que sea titular, sino de ésta en su totalidad».

En el apartado segundo se introdujo una matización, distinguiendo dentro de los datos especialmente protegidos los del artículo 7.2 LOPD (ideología,

---

titular de los datos consienta expresamente y por escrito su divulgación. 3. Con carácter general y, salvo que en el caso concreto prevalezca la protección de datos personales sobre el interés público en la divulgación que lo impidan, se concederá el acceso a información que contenga datos vinculados con la organización, funcionamiento o actividad pública del órgano. 4. Asimismo, se podrá conceder el acceso a información que contenga datos personales que no tengan la consideración de especialmente protegidos si, previa ponderación suficientemente razonada, el órgano competente para resolver considera que no se perjudica ningún derecho constitucionalmente protegido. 5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los datos personales obtenidos a través del ejercicio del derecho de acceso».

[504] El Informe de la Agencia Española de Protección de Datos al Anteproyecto de Ley de Transparencia, acceso a la información pública y buen gobierno, accesible en el siguiente link http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_preceptivos/Administracion_estado/Leyes/common/2012/2013.12.10_2012-0203_APL-Transparencia.pdf

[505] Vid op. cit.

afiliación sindical, religión y creencias), cuyo acceso por terceros solo cabe con el consentimiento expreso y por escrito del afectado, salvo que previamente los haya hecho manifiestamente públicos; y los del artículo 7.3 LOPD (origen racial, salud y vida sexual) o datos relativos a infracciones penales o administrativas que no conllevan amonestación pública al infractor, en cuyo caso el acceso solo se puede autorizar en caso de que se cuente con el consentimiento expreso del afectado o si estuviera amparado por una norma con rango de Ley.

En el apartado tercero dispuso que en el supuesto de los documentos que contengan datos «meramente identificativos» relacionados con la organización, funcionamiento o actividad pública del órgano, con carácter general se concederá el acceso a la información, salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación. Aquí la única adición fue la mención a los datos «meramente identificativos».

En el apartado cuarto, y fuera de estos casos, mantuvo una regla de ponderación del interés público en la divulgación y los derechos de los afectados, en particular su derecho a la protección de datos. Se valió de criterios «por arrastre» derivados de informes previos realizados por la Agencia Española de Protección de Datos sobre materias próximas. En primer lugar. el menor perjuicio de los afectados derivados del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. En segundo lugar, la justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la consideración de investigadores y motiven el acceso en fines históricos, científicos o estadísticos. Finalmente, el tercer y cuarto criterios se refieren al «menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativos de aquéllos» y a «la mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o seguridad». En el apartado quinto se aclaró que no es necesaria esta ponderación si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de

las personas afectadas. Finalmente, en el apartado sexto se mantuvo la previsión de que la normativa sobre protección de datos personales es de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso, que, aunque sea innecesaria, contribuya a reforzar la integración de ambos bloques normativos.

Además, se añadió a sugerencia de la Agencia Española de Protección de Datos una disposición adicional quinta sobre colaboración con la Agencia Española de Protección de Datos, que prevé que ésta y el Consejo de Transparencia y Buen Gobierno, adopten conjuntamente las resoluciones que sean necesarias a fin de determinar los criterios de aplicación de estas reglas, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta norma y en la LOPD.

En las comparecencias ante la Comisión Constitucional, el director de la Agencia Española de Protección de Datos defendió la regulación, como no podía ser de otro modo tratándose de la asunción plena de la propuesta de la Agencia Española de Protección de Datos. Advirtió reiteradamente que la protección de datos no podía servir para denegar automáticamente el acceso ni ser vista como un obstáculo para la transparencia. Apuntó también que los criterios introducidos en el apartado cuarto no eran exhaustivos y cabría introducir otros, como por ejemplo la prevalencia de la publicidad de las informaciones sobre personas que realicen actividades públicas en relación con las mismas. Recomendó, finalmente, la supresión del apartado primero, pues podría ser interpretado como una peor posición del afectado a la información en que figure su nombre que de los terceros (ya que el derecho de acceso de la LOPD tiene un alcance más limitado en su objeto que el de la LTBG).

El profesor SANTAMARIA PASTOR manifestó la necesidad de dar una mayor protección a los datos personales no especialmente protegidos, para salvar la información personal de la mera curiosidad ajena y la pertinencia de exigir, por ello la motivación de las solicitudes y la existencia de un interés legítimo. Por su parte, el profesor GUICHOT puso de relieve el desenfoque

que supone dar entrada como criterios para la ponderación a la consideración de circunstancias referidas al concreto solicitante[506].

3.6.4.2 Normativa aplicable

Una de las enseñanzas del Derecho supranacional y comparado es que la normativa sobre acceso a la información, y no la normativa sobre protección de datos. es de aplicación a las solicitudes de información realizadas por un tercero distinto del afectado[507].

---

[506] Expresamente indicó que se había modificado la regulación de las relaciones entre transparencia y protección de datos, dando entrada a la introducción como criterio de la toma en consideración de la consideración como investigador o de los intereses y derechos que tratan de hacerse valer. «La transparencia y el derecho de acceso a la información es un derecho de ciudadanía al servicio dela democracia. no un derecho instrumental; así lo es en todas las leyes de nuestro entorno. Señorías. sería un error de bulto introducir aquí la referencia a los intereses privados». Por tanto, se deberían eliminar del apartado 4 las letras a) y b) del Anteproyecto de Ley que se basan en esa concepción.

[507] *Vid.* Guichot Reina, E. (2009). *Publicidad y privacidad de la información Administrativa*. Pamplona: Aranzadi. pp. 161-163. «El derecho de acceso a la información en poder de la Administración ha adquirido carta de naturaleza en todos los sistemas analizados, a menudo con referencia constitucional, bien autónoma bien por derivación de la libertad de información. Se vincula con el principio democrático, que exige la transparencia de la actuación pública como forma de implicación y control por parte de los ciudadanos sobre la actuación del poder. A la vez, en todos los sistemas se protege el derecho a la intimidad y a la vida privada. El concepto de intimidad se resiste a ser delimitado de forma precisa y de una vez por todas. Con la aparición de la informática, la protección ha venido a extenderse a todos los datos que dicen relación con una persona física y que, manejados selectivamente o cruzados, pueden condicionar su vida en sociedad. Para ello, además, se han adaptado a esta nueva realidad y ampliado las técnicas puramente defensivas de la intimidad clásica. En esta preocupación está el origen de la acuñación del concepto de «derecho a la protección de datos» como derecho con una regulación autónoma respecto de la intimidad. A partir del postulado según el cual el manejo de cualquier dato, incluso aparentemente intrascendente, puede resultar potencialmente lesivo para el libre desenvolvimiento de la personalidad de los ciudadanos, los Derechos han tendido a extender el concepto de dato personal a cualquier información, del tipo que sea, que lleve asociado el nombre de una persona o pueda a él asociarse. Sin embargo, nos hallamos en un proceso de redefinición de este concepto desvinculado del concepto de vida privada, que por su omnicomprensividad puede llevar a interpretaciones excesivas en detrimento de otros bienes o derechos y muy en especial, a la necesaria circulación de la información en sociedad, en particular, la relativa al ámbito relacional del individuo, esto es, sus actividades profesionales. empresariales o de relación con la Administración Pública. En concreto, y enfrentado al derecho a acceder a la información en poder de la Administración, una concepción tan amplia del ámbito de reserva implicaría la práctica opacidad del actuar administrativo. En todos los Derechos analizados hay una conexión expresa entre la normativa reguladora de la protección de datos y del derecho de acceso, que se resuelve en la aplicación en tanto lex specialis de esta última en los casos de solicitudes de

La precisión es tanto más importante por cuanto la normativa sobre protección de datos contempla un homónimo «derecho de acceso». en el artículo 15 LOPD. Ciertamente difieren los presupuestos —un tratamiento de datos personales desde un fichero–, la titularidad de este derecho –el interesado, entendiendo por tal aquella persona sobre la cual gira la información–, el obligado –el responsable del fichero–, el alcance –información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos presupuestos–, las condiciones de ejercicio y

---

información personal realizadas por terceros. La excepción la constituyen los casos en que el solicitante es el propio afectado, en que la normativa de aplicación es la de protección de datos. Los diversos Derechos estudiados ponen de manifiesto que. en el potencial conflicto entre publicidad y privacidad de la información administrativa, debe prevalecer como regla general el primero cuando se trata de acceder a información relevante para conocer la corrección de la actuación administrativa relativa no a la vida privada de las personas sino a la relación entre el poder público y sus propios empleados, contratistas, agentes, beneficiarios de subvenciones, permisos, etc. Las técnicas para llegar a este resultado son diversas. En unos casos, este tipo de información se excluye *ex lege* del concepto de dato personal a los efectos de la aplicación de la normativa sobre acceso; en otros, la exclusión o el otorgamiento de un escaso peso en la ponderación es fruto de la interpretación de las Autoridades de control y judiciales. Cuando la información se refiere a terceras personas sin un vínculo de especial intensidad con la Administración, es necesario igualmente ponderar entre el interés público de la divulgación de la información y el interés privado en el mantenimiento de la reserva. En la mayoría de los sistemas se veda el acceso a los datos especialmente protegidos en la terminología europea de la protección de datos– o íntimos en sentido clásico, a los que solo puede accederse por vía de requerimiento judicial en el seno de un proceso, salvo que se trate de datos de salud cuyo conocimiento sea necesario para dar respuesta a una urgencia vital para la vida y la integridad de las personas. Los sistemas analizados tienen en común la inclusión de determinaciones adicionales, legales y de creación jurisprudencial, que tienen a maximizar el alcance de ambos derechos, corno el análisis de la posibilidad de anonimizar los documentos si con ello la publicidad no pierde su sentido, de conceder el acceso parcial, de modalizar las formas de acceso para no lesionar el derecho a la privacidad... Una técnica de gran alcance en nuestro tema es la consistente en dar traslado al afectado de la existencia de solicitudes de información que le conciernen, para así poder tomar en consideración con conocimiento de causa la posible lesión en sus derechos e intereses que pudiera causal la divulgación de la información. En todos los casos, la decisión de concesión o denegación del acceso se somete a revisión por Autoridades independientes y a ulterior posibilidad de revisión judicial. Todos los países conocen la existencia de estas Autoridades, coexistiendo dos modelos mayoritarios: una Autoridad independiente sobre acceso a la información y otra sobre protección de datos, coordinadas entre sí en los casos en que se trata de acceder a información personal o bien una Autoridad única».

su garantía –reclamación ante la Agencia de Protección de datos, con un plazo de resolución de seis meses–.

El principio que debe entenderse que rige es el de lex especialis. Se aplicarán a las solicitudes de información la normativa sobre acceso a la información y únicamente será de aplicación de la LOPD y su normativa de desarrollo, cuando el interesado pretende ejercer el derecho de acceso de dicha Ley, con sus diferentes presupuestos y alcance.

3.6.4.3 El acceso a datos especialmente protegidos

La LTBG establece un criterio restrictivo en relación con el acceso a la información que contiene datos especialmente protegidos. Anteriormente se ha apuntado que el artículo 7[508] LOPD considera como tales los relativos a la ideología —incluida la afiliación sindical–, religión o creencias, y solo

---

[508] Artículo 7. Datos especialmente protegidos. «1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento».

pueden ser tratados con el consentimiento expreso y por escrito del afectado. Asimismo, tienen la consideración de datos especialmente protegidos los referidos al origen racial, la salud y a la vida sexual. Éstos solo pueden ser recabados, tratados y cedidos cuando el afectado consienta expresamente (no es necesario en este caso que sea por escrito), o cuando así lo disponga una ley, por razones de interés. La propia LOPD establece excepciones particularizadas al principio de consentimiento expreso referidas a los datos sanitarios. Junto a estos datos se encuentran los relativos a la comisión de infracciones penales o administrativas, a los que alude el mismo artículo para indicar que solo pueden ser incluidos en ficheros públicos, sin dotarles de mayores especificidades.

Este apartado del Anteproyecto[509] fue modificado siguiendo al pie de la letra la propuesta de la Agencia Española de Protección de Datos para armonizarlo al máximo con la LOPD. La redacción inicial establecía un único criterio, según el cual, si la información solicitada contenía datos especialmente protegidos en los términos de la normativa de protección de datos personales, se denegaría el acceso salvo que el titular de los datos consintiera expresamente y por escrito su divulgación.

La actual redacción[510] distingue, siguiendo los postulados del artículo 7 LOPD, entre dos tipos de datos especialmente protegidos. En primer lugar,

---

[509] Artículo 11. Protección de datos personales «2. Si la información solicitada contuviera datos especialmente protegidos en los términos de la normativa de protección de datos personales, se denegará el acceso salvo que el titular de los datos consienta expresamente y por escrito su divulgación».

[510] Artículo 15. Protección de datos personales. «1. Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley. 2. Con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá

los datos relativos a la ideología, religión o creencias. Para cuyo acceso se exige el consentimiento expreso y por escrito del afectado. A menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. En segundo lugar, el caso de los datos de origen racial, salud o vida sexual, o relativos a la comisión de infracciones penales o administrativas que no conlleven la amonestación pública al infractor, respecto de los cuales solo puede autorizarse el acceso con consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley. El precepto sigue también el criterio de la LOPD y, en lo que hace a la publicidad, ya sea activa o pasiva, de las sanciones, aclara que es necesaria una expresa previsión legal, salvo cuando conllevan amonestación pública, puesto estos casos implican de por sí una opción del legislador por la publicidad.

Critica GUICHOT este apartado indicando que lo más cuestionable es el efecto que supone respecto a la inaccesibilidad a la información sobre sanciones administrativas, salvo previsión legal expresa o que se trate de sanciones que conlleven amonestación pública. Información por otra parte que no resulta evidente que pertenezca a la intimidad de las personas, y cuyo conocimiento en ocasiones es crucial para controlar la efectiva

---

el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano. 3. Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal. Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios: a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos. c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos. d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad. 4. No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas. 5. La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso».

aplicación por igual de la ley a todas las personas. Más aun, considerando que incluyen, si se sigue la interpretación que se maneja en el campo de la protección de datos, las sanciones disciplinarias, cuyo conocimiento puede ser de suma relevancia pública para juzgar la actuación administrativa.

3.6.4.4 El acceso a datos meramente identificativos relacionados con la organización, el funcionamiento o actividad pública del órgano

El artículo 15.2 LTBG recoge expresamente que:

> *«con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a información que contenga datos meramente identificativos relacionados con la organización, funcionamiento o actividad pública del órgano».*

Este precepto mantiene la redacción inicial que se establecía en el Anteproyecto, salvo la introducción de la precisión «meramente identificativos». El origen de esta modificación se encuentra en la propuesta por parte de la Agencia Española de Protección de Datos al Anteproyecto. El Reglamento de desarrollo de la LOPD excluyó[511] del concepto de dato personal los meramente identificativos de las personas físicas en cuanto trabajadores, nombre, apellidos, funciones, dirección, teléfono, etc., y los datos de empresarios individuales en su condición de tales.

Sin embargo, el contexto de la transparencia es absolutamente diverso y ajeno a lo que estaba regulado en ese precepto, que tenía como sentido

---

[511] Véase el artículo 2.2 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. «BOE» núm. 17, de 19/01/2008, relativo al ámbito objetivo de aplicación, el cual expresamente reconoce que «este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales».

precisamente aclarar que la presencia del nombre de una persona no puede impedir que se conozcan datos relevantes sobre la actuación pública. No solo datos identificativos de funcionarios o autoridades, sino relativos a las decisiones públicas que adoptan que, a su vez, a menudo, implican la mención de nombres de terceras personas, que pueden ser contratistas, beneficiarios de subvenciones, de licencias, etc.

El sentido de este apartado en el Anteproyecto[512] era exponer cómo ese género de información debía ser, por regla general, pública. Es más, la regulación de la publicidad activa en la LTBG muestra claramente este criterio, con la previsión de publicidad en materia de información institucional y organizativa, incluyendo no solo la identificación de los responsables de los diferentes órganos, sino también su perfil y trayectoria personal[513], sino también, se deberá hacer pública[514], como mínimo, la información relativa a

---

[512] Artículo 11. Protección de datos personales. «3. Con carácter general y, salvo que en el caso concreto prevalezca la protección de datos personales sobre el interés público en la divulgación que lo impidan, se concederá el acceso a información que contenga datos vinculados con la organización, funcionamiento o actividad pública del órgano».

[513] Artículo 6.1 LTBG relativo a la información institucional, organizativa y de planificación, «los sujetos comprendidos en el ámbito de aplicación de este título publicarán información relativa a las funciones que desarrollan, la normativa que les sea de aplicación así como a su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a los responsables de los diferentes órganos y su perfil y trayectoria profesional».

[514] Véase el apartado 1 del artículo 8 LTBG referente a la información económica, presupuestaria y estadística «Los sujetos incluidos en el ámbito de aplicación de este título deberán hacer pública, como mínimo, la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria que se indican a continuación: a) Todos los contratos, con indicación del objeto, duración, el importe de licitación y de adjudicación, el procedimiento utilizado para su celebración, los instrumentos a través de los que, en su caso, se ha publicitado, el número de licitadores participantes en el procedimiento y la identidad del adjudicatario, así como las modificaciones del contrato. Igualmente serán objeto de publicación las decisiones de desistimiento y renuncia de los contratos. La publicación de la información relativa a los contratos menores podrá realizarse trimestralmente. Asimismo, se publicarán datos estadísticos sobre el porcentaje en volumen presupuestario de contratos adjudicados a través de cada uno de los procedimientos previstos en la legislación de contratos del sector público. b) La relación de los convenios suscritos, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, obligados a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas. Igualmente, se publicarán las encomiendas de gestión que se firmen, con indicación de su objeto, presupuesto, duración, obligaciones económicas y las subcontrataciones que se realicen con mención de los adjudicatarios, procedimiento seguido para la adjudicación e importe de la misma. c) Las

los siguientes actos de gestión administrativa con repercusión económica o presupuestaria: i) todos los contratos; ii) la relación de convenios suscritos; iii) las subvenciones y ayudas públicas concedidas; iv) los presupuestos; v) las cuentas anuales; vi) las retribuciones de los altos cargos; vii) las resoluciones sobre compatibilidad; viii) las declaraciones anuales de bienes y actividades; y, ix) la información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia.

Por último, destacar que el artículo 15.2 contiene expresamente una excepción que permite modular los efectos del automatismo, en los siguientes términos «salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida». Y es que puede haber supuestos en que la publicidad de determinada información, incluso meramente identificativa, puede implicar para un individuo, o para un colectivo, un grave perjuicio.

---

subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios. d) Los presupuestos, con descripción de las principales partidas presupuestarias e información actualizada y comprensible sobre su estado de ejecución y sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las Administraciones Públicas. e) Las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo que sobre ellos se emitan. f) Las retribuciones percibidas anualmente por los altos cargos y máximos responsables de las entidades incluidas en el ámbito de la aplicación de este título. Igualmente, se harán públicas las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo. g) Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos así como las que autoricen el ejercicio de actividad privada al cese de los altos cargos de la Administración General del Estado o asimilados según la normativa autonómica o local. h) Las declaraciones anuales de bienes y actividades de los representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares. i) La información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia, en los términos que defina cada administración competente».

3.6.4.5 Ponderación general entre publicidad y protección de datos personales ordinarios

El tercer apartado del artículo 15 declara:

> *«Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada, en particular su derecho fundamental a la protección de datos de carácter personal. Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios: a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos. c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos. d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad».*

La redacción acogida a propuesta de la Agencia Española de Protección de Datos supone una modificación en la redacción del Anteproyecto[515]. La idea inicial era que el criterio de ponderación era el que regía para aquellos casos del apartado segundo del mismo artículo, en que no se tratase de datos

---

[515] Artículo 11. Protección de datos personales «4. Asimismo, se podrá conceder el acceso a información que contenga datos personales que no tengan la consideración de especialmente protegidos si, previa ponderación suficientemente razonada, el órgano competente para resolver considera que no se perjudica ningún derecho constitucionalmente protegido».

personales relacionados con la organización, funcionamiento o actividad pública del órgano. Merece especial atención, y me referiré por ello, a los dos primeros criterios de ponderación. En concreto,

– a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español

Conforme a la letra c) del artículo 57 LPHE, «los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos».

La acogida de este criterio ha sido criticada por la doctrina[516] por varios motivos. En primer lugar, por cuento esos plazos se predican en la Ley del Patrimonio Histórico Español de datos que por su naturaleza pueden calificarse de íntimos o especialmente protegidos y a los que, por ello, no puede accederse sin el consentimiento del interesado, y no para el resto de datos personales. Y ahora, en la LTBG, además, se prevén como de aplicación, no a los datos «íntimos» o «especialmente protegidos», sino a los que no lo son. En segundo lugar, por cuanto se trata de un precepto caracterizado por su ambigüedad. Cabe preguntarse ¿a quién corresponde la acreditación de la fecha de fallecimiento de la persona?

– b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de

[516] Véase, entre otros, Guichot Reina, E. (2014). Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, de 9 de diciembre. Madrid: Tecnos, pp 137-138.

investigadores y motiven el acceso en fines históricos, científicos o estadísticos.

Este apartado ha sido duramente criticado al suponer un torpedo en la línea de flotación del derecho de acceso como derecho autónomo vinculado a la ciudadanía y la igualdad de todos en el conocimiento de la información pública. Supone un desconocimiento grave del sentido del derecho como derecho de ciudadanía para la participación y el control democráticos, dando prevalencia en la ponderación a su uso como instrumento al servicio de la tutela de otros derechos individuales o introduciendo diferencias de trato en función de la cualidad del solicitante y de justificación de intereses particulares ajenos a la lógica del derecho y del resto del articulado de la LTBG, que excluye expresamente la necesidad de acreditan interés alguno o de motivar las solicitudes[517].

Además, una vez facilitado el acceso a la información a cualquier solicitante, éste puede hacerla circular libremente a personas en quienes no concurran la condición de investigadores.

3.6.4.6 La disociación

El apartado cuarto del artículo 15 LTBG aclara que:

> *«No será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas».*

En realidad, una primera aproximación nos podría hacer pensar que este apartado es tautológico, por cuanto en ese caso, la información deja de contener datos personales. Ya hemos visto que el apartado a) del artículo 3

[517] Guichot Reina E. (2012). El Proyecto de Ley de Transparencia y acceso a la información pública y el margen de actuación de las Comunidades Autónomas. *Revista Andaluza de Administración Pública, 84*. Sevilla: IAAP, pp 121-122.

de la LOPD entiende por tales «cualquier información concerniente a personas físicas identificadas o identificables».

En muchas ocasiones, bastará la disociación para conseguir un correcto equilibrio entre transparencia y protección de datos, aunque hay que estar a cada caso ya que, en función de lo singular de la información, en ocasiones las personas a las que van referidas siguen siendo identificables[518]. La Agencia de Protección de Datos ha requerido en sus Resoluciones que esa disociación ha de ser irreversible. Sin embargo, como digo, y comprobaremos posteriormente, no siempre se consigue.

3.6.4.7 La aplicación posterior de la normativa sobre protección de datos

Tal y como recoge el último apartado del artículo 15 LTBG,

> *«la normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso».*

Ahora bien, dicha normativa tiene como presupuesto la integración de los datos en ficheros y su tratamiento, es decir que, fuera de esos presupuestos, no cabe invocar a normativa sobre protección de datos para impedir la divulgación general por el solicitante de la información obtenida conforme a la LTBG.

Lo principal en este artículo 15.5 es la referencia al término «tratamiento». Aunque posteriormente incidiremos sobre ello, basta con señalar que la letra c) del artículo 3 LOPD define el tratamiento de datos como aquellas «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias». Así, bastaría

---

[518] En efecto, y así lo explicaré posteriormente, es posible la utilización de diferentes tratamientos a los datos de carácter personal disociados, los cuales, en la práctica, reviertan esa cualidad. Estoy haciendo referencia a la computación ubicua, lo cual nos traslada a uno de los problemas actuales, pues tiene repercusión directa en el principio del consentimiento.

con no hacer nada de estas operaciones con la información a la que hemos accedido, para que no se aplique la LOPD.

3.6.4.8 La colaboración con la autoridad de protección de datos

A sugerencia de la Agencia Española de Protección de Datos se añadió al proyecto de LTBG lo que con posterioridad se convertiría en la disposición adicional quinta[519] sobre colaboración con la Agencia Española de Protección de Datos. En ésta se prevé que el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adopten conjuntamente las resoluciones que sean necesarias a fin de determinar los criterios de aplicación de estas reglas, en particular, lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en la LTBG y en la LOPD.

En los países donde existe el modelo de doble agencia implantado en España, como Portugal, Italia o Francia, las relaciones entre ambas han estado tradicionalmente marcadas por cierta tensión y disparidad de criterios.

No debemos olvidar, ni obviar, que es la normativa sobre acceso la que rige la publicidad activa o pasiva de información que contiene datos de terceros, y en ese sentido, siendo deseable una interpretación armónica de ambos bloques normativos, dicha interpretación ha sido la efectuada por el legislador en el artículo 15 LTBG, y su interpretación, como la del resto de su articulado, es competencia de las autoridades de transparencia

---

[519] Disposición adicional quinta. Colaboración con la Agencia Española de Protección de Datos. «El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre».

4 EFECTIVIDAD DE LA TRANSPARENCIA: PUBLICIDAD ACTIVA Y PUBLICIDAD PASIVA

Para cumplir las funciones democráticas y del Estado de Derecho, la transparencia administrativa tiene que ser efectiva. No es suficiente dar al ciudadano la mera posibilidad o el mero derecho de informarse sobre la actuación administrativa, sino que hacer falta hacer comprensible los procesos de toma de decisión y los argumentos relevantes a favor y en contra para facilitar al particular una formación de opinión propia.

Una transparencia activa presupone una iniciativa propia de la Administración para hacer comprensible la actuación administrativa, tanto a la hora de mostrar al interesado en un caso concreto sus opciones correspondientes de actuar y de defenderse, como cuando se trata de informar al público sobre asuntos de interés general. Aunque no se puede forzar a los ciudadanos a interesarse o a participar en los procesos de formación de la voluntad, sí se puede ofrecer información y de esta manera disminuir el umbral de comunicación.

La necesidad de atribuir a la Administración Pública un papel activo en proporcionar información y explicaciones crece en la medida que la complejidad de la decisión en cuanto a los actores involucrados, a los criterios de Derecho aplicables y a los intereses en juego aumenta.

Desde la perspectiva de los particulares, la posibilidad de conseguir una información diferenciada y al mismo tiempo comprensible, puede aumentar la confianza en la racionalidad del proceso de formación de la voluntad.

4.1 Publicidad Activa

En la actual sociedad, en la que hemos incorporado Internet a nuestra vida diaria, un alto grado de transparencia en la gestión de los asuntos públicos es universalmente entendido como una exigencia democrática. Las autoridades deben poner la información a disposición de todos motu propio, sin esperar el planteamiento de solicitudes individuales. En especial, aquélla

más relevante para alcanzar la finalidad para la que nació el derecho de acceso a la información: posibilitar el conocimiento, la participación y el control de las personas sobre los asuntos públicos.

Antes de la LTBG, el artículo 37.9[520] LRJPAC obligaba a publicar relaciones documentales, si bien dejaba en una casi total indeterminación a qué tipo de publicación se refería, qué información abarcaba, con qué periodicidad o cuáles eran las vías de impugnación en caso de incumplimiento. El apartado 10[521] del mismo artículo, refería la publicación a circulares e instrucciones de aplicación del derecho, pero no a actos referentes a la organización y funcionamiento internos de la Administración.

4.1.1 Derecho supranacional y comparado

En el Derecho comparado, las leyes de acceso a la información han ido acogiendo el principio general de publicidad activa de la información más relevante para posibilitar la participación y control de la gestión pública. En algunos casos, se dispone, además, la publicación de la información que haya sido ya objeto de una o varias solicitudes previas.

Afirma BARRERO RODRÍGUEZ que, en muchas ocasiones, un registro de documentos que permite conocer qué información se encuentra en poder de la autoridad pública y que admite la búsqueda con diferentes criterios, y una vez localizada, la posibilidad de poder acceder al texto completo a golpe de click. Este nuevo y revolucionario medio de comunicación está llamado a sustituir en buena medida al mecanismo de la información previa solicitud –o «publicidad pasiva»– y posibilitando un acceso inmediato y universal,

---

[520] «Artículo 37. Derecho de acceso a Archivos y Registros. 9. Será objeto de periódica publicación la relación de los documentos obrantes en poder de las Administraciones Públicas sujetos a un régimen de especial publicidad por afectar a la colectividad en su conjunto y cuantos otros puedan ser objeto de consulta por los particulares»

[521] «Artículo 37. Derecho de acceso a Archivos y Registros. 10. Serán objeto de publicación regular las instrucciones y respuestas a consultas planteadas por los particulares u otros órganos administrativos que comporten una interpretación del derecho positivo o de los procedimientos vigentes a efectos de que puedan ser alegadas por los particulares en sus relaciones con la Administración».

generando con ello un ahorro de costes y potenciando una buena gestión pública de la información[522].

La publicidad activa puede contribuir también a la generación de nueva información y de servicios de valor añadido puestos a disposición de la sociedad, tanto empresariales como de organizaciones no gubernamentales e iniciativas particulares que explotan datos con fines de denuncia, debate social, etc. Se trata de cruzar datos de distinta procedencia e inventar nuevas aplicaciones que a su vez puedan redundar en una mejor información a disposición de las autoridades públicas que le permita mejorar sus políticas y adaptarlas a las necesidades ciudadanas, así como detectar las disfunciones.

Es esta idea, que conecta con la idea de gobernanza y de gobierno abierto y colaborativo, la que está detrás de los proyectos llamados de open data. Estos proyectos plantean el reto de garantizar la preservación de los intereses protegidos por las limitaciones acogidas en las leyes de acceso, teniendo en cuenta los nuevos riesgos que puede generar el cruce de datos y la generación de nuevas aplicaciones, a partir de informaciones en principio «inofensivas», en una preocupación similar a la que dio lugar a la diferenciación del concepto de intimidad y el más extenso de protección de datos.

En efecto, se apuntan como riesgos de la puesta a disposición indiscriminada de datos la posibilidad de malas interpretaciones o de informaciones parciales o sesgadas[523], e incluso de afectación a valores fundamentales de la vida en sociedad.

---

[522] Barrero Rodríguez, M.C. (2014). Publicidad Activa. En Guichot Reina, E. (Coord). *Transparencia, acceso a la información pública y buen gobierno. Estudio de la Ley 19/2013*, de 9 de diciembre. Madrid: Tecnos. p.146.

[523] La información tiene valor para los ciudadanos cuando es relevante, complete y comprensible. Véase Lessig, L. (2009). Against transparency, *The New Republic.* En https://newrepublic.com/article/70097/against-transparency

En el Derecho comunitario y en muchos Derechos estatales, un elemento fundamental para este cometido son los registros públicos. En efecto, junto con la virtud de dar a conocer de qué información se dispone, sus efectos favorecedores del conocimiento de la información pública se multiplican si se tiene en cuenta que una parte sustancial de los documentos que constan en los registros son directamente accesibles en su texto íntegro, a través de un hipervínculo. Es el llamado «acceso directo»[524].

4.1.2 Principios generales.

4.1.2.1 La evolución del texto durante la tramitación de la Ley

El primer Anteproyecto de la LTBG previó la publicación periódica y actualizada de la información cuyo conocimiento fuera relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública. Aclaró que sin de aplicación, en su caso, los límites de acceso a la información, en especial el relativo a la protección de datos.

El segundo Anteproyecto añadió que la información sujeta a las obligaciones de transparencia será publicada en las correspondientes sedes electrónicas o páginas web y de una manera clara, estructurada y entendible para los interesados, y preferiblemente, en formato reutilizable. Añadió que se establecerán los mecanismos adecuados para facilitar la accesibilidad, la interoperabilidad, la calidad y la reutilización de la información publicada, así como su identificación y localización.

Por su parte, y en relación a los límites de la publicidad activa, el Informe de la Agencia Española de Protección de Datos recomendó añadir la referencia

---

[524] En la normativa comunitaria se prevé la publicación en el Diario Oficial de toda una serie de documentos sobre los que hasta su entrada en vigor no existía dicha obligación, ya estén relacionados con la actividad prelegislativa, sean actos programáticos o no vinculantes. De este modo, una gran parte de los documentos para cuyo acceso con anterioridad había que cursar una solicitud, están hoy disponibles con carácter general para el público, a través del Diario Oficial que, a su vez, es objeto de publicación electrónica. La importancia de la transparencia alcanza su cumbre en el proceso legislativo, en el que se conforman las decisiones fundamentales de la vida social.

expresa que «cuando la información contuviera datos especialmente protegidos, la publicidad solo se llevará a cabo previa disociación de los mismos»[525].

4.1.2.1.1 Alcance de la información sometida a publicidad activa

En el artículo 5.1 de la LTBG se establece como principio general la publicación de forma periódica y actualizada de la información «cuyo conocimiento sea relevante para garantizar la transparencia de su actividad relacionada con el funcionamiento y control de la actuación pública».

Afirma BARRERO RODRÍGUEZ que es de aplaudir que el legislador haya previsto todo un elenco de materias que merecen esa consideración. Sin embargo, se ha de entender que el listado de los artículos 6 a 8 es un listado de mínimos, de información que el legislador ha considerado relevante, y que debe de ampliarse a toda materia que juzguen relevante para el conocimiento público, siempre y cuando se respeten los límites establecidos en los artículos 14 y 15. Este listado de mínimos, dotado de carácter básico, se podría ampliar por posteriores normas estatales o, en ámbito de aplicación por normas autonómicas[526].

4.1.2.1.2 Forma de publicación

Los apartados cuarto y quinto del artículo 5 LTBG se refieren a la forma de publicidad de la información caracterizadas por:

Toda la información será comprensible, de acceso fácil, universal, gratuito e interoperable[527], lo que implica un diseño técnico que lo permita.

---

[525] Véase el «Informe de la Agencia Española de Protección de Datos al Anteproyecto de Ley de Transparencia, acceso a la información pública y buen gobierno», pp. 37-38. Accesible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_preceptivos/Administracion_estado/Leyes/common/2012/2013.12.10_2012-0203_APL-Transparencia.pdf

[526] Barrero Rodríguez, M.C. (2014). Publicidad Activa. En Guichot Reina, E. (Coord). *Transparencia, acceso a la información pública y buen gobierno. Estudio de la Ley 19/2013*, de 9 de diciembre. Madrid: Tecnos. pp. 153-154.

[527] La «interoperabilidad» es la capacidad de los sistemas de información y de los procedimientos a los que éstos dan soporte, de compartir datos y posibilitar el intercambio de información y

Se establecerán los mecanismos para facilitar la accesibilidad, la calidad, así como su identificación y localización, lo que parece exigir que esté clasificada y ordenada temáticamente, permita la localización a través de un buscador avanzado y que, al menos, esté rotulada de forma que permita entender el tipo de información al que se está accediendo.

Publicada en formatos preferiblemente reutilizables. Este apartado plantea la cuestión de cuál es la conexión de la LTBG y la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, cuyo artículo 7[528] permite someter a tasa o precio público la entrega de documentos para fines comerciales o no comerciales.

---

conocimiento entre ellos. El contenido de esta definición se ha obtenido en: https://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Interoperabilidad_Inicio.html

[528] El artículo 7 de la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público, «BOE» núm. 276, de 17 de noviembre de 2007, se refiere al régimen jurídico de las tarifas en los siguientes términos «1. Podrá aplicarse una tarifa por el suministro de documentos para su reutilización en las condiciones previstas en la normativa estatal vigente o, en su caso, en la normativa que resulte de aplicación en el ámbito autonómico o local, limitándose la misma a los costes marginales en que se incurra para su reproducción, puesta a disposición y difusión. En el caso de las publicaciones oficiales electrónicas con precio de venta al público, se aplicará, al menos, el mismo precio privado de la Administración establecido como precio de venta. 2. Lo dispuesto en el apartado anterior no se aplicará a: a) Los organismos del sector público a los que se exija generar ingresos para cubrir una parte sustancial de sus costes relativos a la realización de sus misiones de servicio público. b) A título de excepción, los documentos para los cuales se exija a los organismos del sector público en cuestión que generen ingresos suficientes para cubrir una parte sustancial de los costes de recogida, producción, reproducción y difusión de documentos. Estos requisitos se fijarán de antemano y se publicarán por medios electrónicos siempre que sea posible y apropiado. c) Las bibliotecas, incluidas las universitarias, los museos y los archivos. 3. En los casos a los que se hace referencia en el apartado 2, letras a) y b), los organismos del sector público en cuestión, calcularán el precio total conforme a criterios objetivos, transparentes y comprobables, que serán fijados mediante la normativa que corresponda. Los ingresos totales de estos organismos obtenidos por suministrar documentos y autorizar su reutilización durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción y difusión, incrementado por un margen de beneficio razonable de la inversión. La tarifa se calculará conforme a los principios contables aplicables a los organismos del sector público correspondientes, y de acuerdo con la normativa aplicable. 4. Cuando sean los organismos del sector público mencionados en el apartado 2, letra c), los que apliquen tarifas, los ingresos totales obtenidos por suministrar y autorizar la reutilización de documentos durante el ejercicio contable apropiado no superarán el coste de recogida, producción, reproducción, difusión, conservación y compensación de derechos, incrementado por un margen de beneficio razonable de la inversión. A los efectos de calcular dicho margen, estos organismos podrán tener en cuenta los precios

Sin embargo, se ha de aclarar desde este mismo momento que esta última Ley, no se apoya, pese a su título, en el concepto de información sino en el documento. La información sobre las materias objeto de publicidad activa no se refiere a documentos, y no implica necesariamente que se adjunte un enlace para la consulta directa de los documentos de los que la información trae causa, que podrá hacerse o no, y que en todo caso podrán ser solicitados en ejercicio del derecho de acceso.

4.1.3 Información institucional, organizativa y de planificación

4.1.3.1 Consideración general

El artículo 6[529] LTBG impone a todos «los sujetos comprendidos en el ámbito de aplicación de este Título», la obligación de ofrecer «información institucional, organizativa y de planificación».

---

aplicados por el sector privado por la reutilización de documentos idénticos o similares. Las tarifas se calcularán conforme a los principios contables aplicables a los organismos del sector público correspondientes y de acuerdo con la normativa aplicable. 5. Se podrán aplicar tarifas diferenciadas según se trate de reutilización con fines comerciales o no comerciales. 6. Las Administraciones y organismos del sector público publicarán por medios electrónicos, siempre que sea posible y apropiado, las tarifas fijadas para la reutilización de documentos que estén en poder de organismos del sector público, así como las condiciones aplicables y el importe real de los mismos, incluida la base de cálculo utilizada. En el resto de los casos en que se aplique una tarifa, el organismo del sector público de que se trate indicará por adelantado qué factores se tendrán en cuenta para el cálculo de la misma. Cuando se solicite, dicho organismo también indicará cómo se han calculado esa tarifa en relación con la solicitud de reutilización concreta. No obstante, lo dispuesto en el párrafo anterior podrá no ser de aplicación en el caso de las bibliotecas (incluidas las universitarias) museos y archivos, a la hora de fijar sus tarifas. 7. Cuando las tarifas a exigir tengan la naturaleza de tasa, su establecimiento y la regulación de sus elementos esenciales se ajustarán a lo previsto en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, y demás normativa tributaria».

[529] «Artículo 6. Información institucional, organizativa y de planificación. 1. Los sujetos comprendidos en el ámbito de aplicación de este título publicarán información relativa a las funciones que desarrollan, la normativa que les sea de aplicación así como a su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a los responsables de los diferentes órganos y su perfil y trayectoria profesional. 2. Las Administraciones Públicas publicarán los planes y programas anuales y plurianuales en los que se fijen objetivos concretos, así como las actividades, medios y tiempo previsto para su consecución. Su grado de cumplimiento y resultados deberán ser objeto de evaluación y publicación periódica junto con los indicadores de medida y valoración, en la forma en que se determine por cada Administración competente. En el ámbito de la Administración

Nos encontramos ante un conjunto de deberes de publicidad activa que no pueden considerarse una novedad en nuestro Derecho. El valor de lo dispuesto en este artículo se encuentra en su generalización, con carácter básico, a todas las Administraciones Públicas y en la extensión de alguna de las obligaciones que prevé a otras entidades tanto públicas como privadas, al margen hasta ahora, de exigencias de esta naturaleza.

El artículo 6.2 añade otras obligaciones que vinculan solo a las Administraciones Públicas. Así, éstas han de publicar «los planes y programas anuales y plurianuales en los que se fijen objetivos concretos, así como las actividades, medios y tiempo previsto para su consecución. Su grado de cumplimiento y resultados deberán ser objeto de evaluación y publicación periódica junto con los indicadores de medida y valoración, en la forma en que se determine por cada Administración competente».

Fue el Consejo de Estado el que sugirió en su Dictamen 707/2012[530], que se introdujera «la obligación de publicar los resultados de la evaluación relativa al grado de cumplimiento de los planes y programas», a fin de intensificar el régimen de transparencia contenido en el precepto.

Finalmente, el artículo 6 LTBG no ha incorporado a su listado de obligaciones de publicidad activa otros contenidos posibles. Es lo que ocurre señaladamente con las agendas de reuniones de Ministros y altos cargos, que había sido solicitada reiteradamente.

Sin embargo, el Consejo de Transparencia y Buen Gobierno ha dictado la Recomendación 1/2017 sobre información de las Agendas de los

---

General del Estado corresponde a las inspecciones generales de servicios la evaluación del cumplimiento de estos planes y programas»

[530]Consejo de Estado (2012). Informe 707/2012 al Anteproyecto de Ley de Transparencia, acceso a la información pública y buen gobierno, de 19 de julio de 2012. En http://www.boe.es/buscar/doc.php?id=CE-D-2012-707. «Desde otra perspectiva, cabe apuntar que el régimen de transparencia contenido en este precepto podría intensificarse introduciendo la obligación de publicar los resultados de la evaluación relativa al grado de cumplimiento de los planes y programas anuales y plurianuales prevista en el apartado dos in fine».

responsables públicos[531]. En éste, y recogiendo las palabras del Preámbulo de la Ley LTBG:

> *«Solo cuando la acción de los responsables públicos se somete a escrutinio, cuando los ciudadanos pueden conocer cómo se toman las decisiones que les afectan, cómo se manejan los fondos públicos o bajo qué criterios actúan nuestras instituciones podremos hablar del inicio de un proceso en el que los poderes públicos comienzan a responder a una sociedad que es crítica, exigente y que demanda participación de los poderes públicos».*

Declara expresamente que su carácter de información pública es indudable, y en este sentido, «considera necesario determinar cuáles son los datos y la información relativos a las reuniones, visitas y actividades de los miembros del Gobierno y los altos cargos de la AGE que constituyen información pública y por lo tanto, deberían hacerse públicas, y en qué términos sería conveniente proceder a su publicación y facilitar su acceso a la información. Además, se considera conveniente definir el contenido de la que podría denominarse "Agenda para la Transparencia" de los responsables públicos, destinada a ser publicada proactivamente para facilitar la rendición de cuentas y garantizar, además, la unidad, coherencia y tratamiento de la información».

Así, continúa el Consejo indicando que «esta demanda y el interés que manifiesta, entroncan directamente con el objetivo último con el que fue aprobada la Ley de Transparencia y con el interés legítimo de los ciudadanos en la rendición de cuentas y favorece el escrutinio de la actividad pública. El conocimiento de las agendas de los responsables públicos ayuda a alcanzar este objetivo y su contenido constituye, con carácter general, información que entra dentro del ámbito de aplicación de la normativa sobre acceso a la información pública, en la medida en que obran en poder de

---

[531] El contenido de la Recomendación se puede consultar en el siguiente link http://www.consejodetransparencia.es/ct_Home/dms/ctransp/consejo/informes_consultas_criterios/recomendaciones/Recomendacion-1_2017_agendas/Recomendacion%201_2017_agendas.docx

organismos públicos sujetos a la Ley. Es decir, constituye información pública a los efectos del artículo 13 de la LTBG. En consecuencia, la información referida a la actividad de quienes dirigen, organizan y son responsables de la toma de decisiones, contribuye a formar en la ciudadanía un mejor conocimiento de la actividad pública y, con ello, a facilitar el escrutinio ciudadano y el ejercicio del control democrático […] La información acerca de la actividad pública diaria de los responsables públicos -siempre que tenga trascendencia pública y con exclusión, por tanto, de aquella estrictamente relacionada con el funcionamiento interno o cotidiano de los correspondientes organismos-, debe ser publicada con la mayor extensión posible y sin perjuicio de la aplicación de los límites establecidos en la LTBG entendidos según lo previsto en la norma y de acuerdo con la interpretación restrictiva que de los mismos realiza este Organismo y los Tribunales de Justicia.

El Consejo entiende, asimismo, que el objeto de esta publicación debe ser la agenda[532] de trabajo del responsable público como reflejo de su desempeño diario y del ejercicio de sus competencias, funciones y tareas».

---

[532] El artículo tercero de la Recomendación se refiere al contenido de la Agenda para la transparencia. Así, «A los efectos de esta Recomendación se entiende por agenda la relación ordenada de asuntos, compromisos o quehaceres asumidos por los altos cargos y máximos responsables según lo indicado en la disposición anterior en un período de tiempo determinado, soportada en libros, cuadernos, dispositivos electrónicos o cualquier otro medio que sirva para anotar, tener constancia o hacer seguimiento de los temas o asuntos que se traten. A los mismos efectos, en el marco de la agenda definida en el apartado anterior, serán Agendas para la Transparencia las que reflejen la actividad pública de los sujetos incluidos en la presente recomendación, es decir, aquella parte de su actividad relacionada con la toma de decisiones en las materias de su competencia, la gestión y manejo de fondos o recursos públicos y la delimitación de criterios de actuación. Las Agendas para la Transparencia, como expresión de la rendición de cuentas, tienen la consideración de información pública de acuerdo con lo dispuesto en la LTBG y permiten el escrutinio del desempeño de las funciones públicas y de las acciones que desarrollen los sujetos obligados conforme al Preámbulo de la LTBG. Las Agendas para la Transparencia serán objeto de publicación en los términos establecidos en la Disposición quinta».

4.1.4 Información de relevancia jurídica

El artículo 7[533] determina la «información de relevancia jurídica» que han de ofrecer las Administraciones Públicas.

4.1.5 Información económica, presupuestaria y estadística

La categoría referida a la información económica, presupuestaria y estadística, acogida en el artículo 8[534] LTBG, es quizás, la más compleja de

---

[533] Artículo 7. Información de relevancia jurídica. «Las Administraciones Públicas, en el ámbito de sus competencias, publicarán: a) Las directrices, instrucciones, acuerdos, circulares o respuestas a consultas planteadas por los particulares u otros órganos en la medida en que supongan una interpretación del Derecho o tengan efectos jurídicos. b) Los Anteproyectos de Ley y los proyectos de Decretos Legislativos cuya iniciativa les corresponda, cuando se soliciten los dictámenes a los órganos consultivos correspondientes. En el caso en que no sea preceptivo ningún dictamen la publicación se realizará en el momento de su aprobación. c) Los proyectos de Reglamentos cuya iniciativa les corresponda. Cuando sea preceptiva la solicitud de dictámenes, la publicación se producirá una vez que estos hayan sido solicitados a los órganos consultivos correspondientes sin que ello suponga, necesariamente, la apertura de un trámite de audiencia pública. d) Las memorias e informes que conformen los expedientes de elaboración de los textos normativos, en particular, la memoria del análisis de impacto normativo regulada por el Real Decreto 1083/2009, de 3 de julio. e) Los documentos que, conforme a la legislación sectorial vigente, deban ser sometidos a un período de información pública durante su tramitación».

[534] Artículo 8. Información económica, presupuestaria y estadística. «1. Los sujetos incluidos en el ámbito de aplicación de este título deberán hacer pública, como mínimo, la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria que se indican a continuación: a) Todos los contratos, con indicación del objeto, duración, el importe de licitación y de adjudicación, el procedimiento utilizado para su celebración, los instrumentos a través de los que, en su caso, se ha publicitado, el número de licitadores participantes en el procedimiento y la identidad del adjudicatario, así como las modificaciones del contrato. Igualmente serán objeto de publicación las decisiones de desistimiento y renuncia de los contratos. La publicación de la información relativa a los contratos menores podrá realizarse trimestralmente. Asimismo, se publicarán datos estadísticos sobre el porcentaje en volumen presupuestario de contratos adjudicados a través de cada uno de los procedimientos previstos en la legislación de contratos del sector público. b) La relación de los convenios suscritos, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, obligados a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas. Igualmente, se publicarán las encomiendas de gestión que se firmen, con indicación de su objeto, presupuesto, duración, obligaciones económicas y las subcontrataciones que se realicen con mención de los adjudicatarios, procedimiento seguido para la adjudicación e importe de la misma. c) Las subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios. d) Los presupuestos, con descripción de las principales partidas presupuestarias e información actualizada y comprensible sobre su estado de ejecución y sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las Administraciones Públicas. e) Las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización

la llamada publicidad activa, habida cuenta de que se trata básicamente de materias de contenido económico y presupuestario, que hacen relación a la disposición de los fondos públicos o versan sobre la situación económica de los responsables de la gestión pública, y por tanto un ámbito donde la información siempre ha sido más demandada por la ciudadanía.

Se trata de poder acceder, en las páginas web y sedes electrónicas de las organizaciones que gestionan recursos públicos, a la información que permita verificar a qué actividades se destinan los fondos públicos y poder saber también si la gestión administrativa con repercusión económica o presupuestaria ha sido eficiente y eficaz. La transparencia se convierte en una medida de prevención o disuasión de actuaciones poco convenientes y, desde luego, en un medio o instrumento necesario para un control de la gestión pública por parte de la ciudadanía.

El artículo 8 LTBG establece cuáles son las materias relativas a los actos de gestión administrativa con repercusión económica o presupuestaria que deben ser necesariamente objeto de publicidad activa, especificando en sus

---

por parte de los órganos de control externo que sobre ellos se emitan. f) Las retribuciones percibidas anualmente por los altos cargos y máximos responsables de las entidades incluidas en el ámbito de la aplicación de este título. Igualmente, se harán públicas las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo. g) Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos, así como las que autoricen el ejercicio de actividad privada al cese de los altos cargos de la Administración General del Estado o asimilados según la normativa autonómica o local. h) Las declaraciones anuales de bienes y actividades de los representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares. i) La información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia, en los términos que defina cada administración competente. 2. Los sujetos mencionados en el artículo 3 deberán publicar la información a la que se refieren las letras a) y b) del apartado primero de este artículo cuando se trate de contratos o convenios celebrados con una Administración Pública. Asimismo, habrán de publicar la información prevista en la letra c) en relación a las subvenciones que reciban cuando el órgano concedente sea una Administración Pública. 3. Las Administraciones Públicas publicarán la relación de los bienes inmuebles que sean de su propiedad o sobre los que ostenten algún derecho real».

distintos apartados y subapartados el alcance de la información que, como mínimo, deberá publicarse.

Incrementar la transparencia en relación con la contratación del sector público ha estado presente desde los primeros momentos en que se abordó la necesidad de una Ley de transparencia y acceso a la información.

El interés de la ciudadanía por saber el estado de las cuentas públicas es constante y desde luego, toda vez que se hace casi imperioso acceder a una información que permita un conocimiento certero de a qué se destinan los fondos públicos y, con ello, los tributos. Si es legítimo que todos sostengan las necesidades públicas, no lo es menos que se tenga conocimiento de cómo se emplean los recursos y cuál ha sido la gestión de los mismos. En el Congreso se dio nueva redacción al precepto, especificando, de un lado, que la información sobre su estado de ejecución debe ser actualizada y comprensible, y, de otro, añadiendo la información sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las Administraciones Públicas.

La letra e) del artículo 8.1 prevé la publicidad de «las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo que sobre ellos se emitan». Si se tiene en cuenta que el presupuesto que el presupuesto es en realidad una estimación más o menos acertada de las previsiones de ingresos y gastos de las organizaciones públicas, se comprende que, al final del ejercicio, estas previsiones pueden haber sufrido modificaciones y que su ejecución evidencie que la realidad pueda no ser la inicialmente estimada.

Por esta razón, para poder conocer la realidad de las cuentas públicas, la información completa de los ocurrido en el ejercicio se desplaza a otro documento: el estado de las cuentas anuales, donde ya se detallan de manera fiel cuáles han sido los ingresos y gastos efectivamente acaecidos. Es más, la noción o categoría de rendición de cuentas de los sujetos públicos hace relación directa con este apartado, con las cuentas anuales. Desde esta consideración, es de alabar que la LTBG haya recogido la obligación

de publicarlas en las sedes electrónicas y páginas web de las entidades a las que se aplica.

Sin embargo, no han prosperado las propuestas dirigidas a extender esta obligación de publicidad a cualquier entidad privada que reciba fondos públicos. Y creemos que no está justificado, toda vez que la naturaleza pública del dinero recibido justifica que se deba detallar el destino que ha tenido, de forma accesible a la ciudadanía.

Por último, señalar que la obligación de publicidad se extiende a la información estadística que permita valorar el grado de cumplimiento y calidad de los servicios públicos y, por consiguiente, exige que se elaboren dichas estadísticas, pero los términos en que se satisface tal obligación, quedan remitidos al criterio de la administración competente, entendiendo por tal a la titular del servicio público de que se trate.

4.2 El derecho de acceso a la información. Publicidad pasiva

4.2.1 La información pública como objeto del derecho de acceso

El artículo 12[535] LTBG reconoce a todas las personas «el derecho a acceder a la información pública en los términos previstos en el artículo 105. b) de la Constitución Española, desarrollados por esta Ley». El objeto del derecho es la información, lo que constituye una importante novedad dado que, hasta esta Ley, eran siempre los documentos.

Así, el artículo 37.1[536] LRJPAC, antes de su reforma por la LTBG, reconocía el derecho de acceso a los registros y documentos «que, formando parte de un expediente, obren en los archivos administrativos».

---

[535] Artículo 12. Derecho de acceso a la información pública. «Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105.b) de la Constitución Española, desarrollados por esta Ley. Asimismo, y en el ámbito de sus respectivas competencias, será de aplicación la correspondiente normativa autonómica».

[536] Artículo 37. Derecho de acceso a Archivos y Registros. «1. Los ciudadanos tienen derecho a acceder a los registros y a los documentos que, formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de

Se entiende por información pública «los contenidos o documentos, cualquiera que sea su formato o soporte que obren en poder de alguno de los sujetos incluidos en el ámbito de aplicación de este Título y que hayan sido elaborados o adquiridos en el ejercicio de sus funciones»[537].

4.2.2 La concreción de la información desde el punto de vista objetivo

4.2.2.1 Los «documentos» y «contenidos» en el artículo 13 LTBG

La ley no nos ofrece un concepto de documento, lo que sin duda hubiera resultado oportuno[538]. Sí lo hacía, a los concretos efectos del derecho de acceso, el artículo 37 LRJPAC en su redacción originaria, refiriéndolo a los que «formando parte de un expediente, obren en los archivos administrativos, cualquiera que sea la forma de expresión, gráfica, sonora o en imagen o el tipo de soporte material en que figuren»[539].

---

soporte material en que figuren, siempre que tales expedientes correspondan a procedimientos terminados en la fecha de la solicitud».

Como es sabido, la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, ha sido derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. De esta forma, la redacción del artículo comentado, se ha trasladado al apartado c) del artículo 13 de esta última norma, siendo su contenido «Artículo 13. Derechos de las personas en sus relaciones con las Administraciones Públicas. Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos: […] d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico».

[537] Véase el artículo 13 LTBG referente al concepto de información pública.

[538] De hecho, la Asociación de Archiveros Españoles en la Función Pública en sus Propuestas al Anteproyecto así lo requirió al Gobierno. Proponían la siguiente definición: «se entiende por documento público toda la información producida o recibida por las personas físicas o jurídicas, tanto públicas como privadas, enumeradas en el ejercicio de las competencias que les son propias como testimonio de sus actos, recogida en un soporte, con independencia de la forma de expresión o contexto tecnológico en que se haya generado y elaborado de acuerdo con unas características de tipo material y formal».

[539] Sobre el concepto de documento en esta disposición, véase Rams Ramos, L. (2008). *El derecho de acceso a archivos y registros administrativos*. Madrid: Reus, pp. 387-401.

En definitiva, el documento es el objeto de cualquiera naturaleza que exterioriza un pensamiento humano a través de la escritura o de cualquier otro signo. No existen razones para pensar que no sea éste el concepto que recoge el artículo 13 LTBG.

Las dificultades surgen en la concreción de esos «contenidos» que acompañan a los documentos en la definición de la información que ofrece el artículo 13 LTBG. Afirma BARRERO RODRÍGUEZ que quizá la concreción de este concepto, «contenidos», pueda ofrecerse a partir de una de las características básicas y consustanciales al documento: su accesibilidad. Esto es, el documento supone la incorporación de la información a un soporte perdurable y, por definición, accesible. Desde esta base, es posible que esos «contenidos» a los que se refiere a la Ley, no sean más que aquellos otros objetos que aportan una información a la que, a diferencia del documento, no es posible acceder sin su previo tratamiento por los sujetos obligados a facilitarla[540].

En definitiva, puede entenderse que el artículo 13 LTBG reconoce un derecho de acceso tanto a la información accesible en el momento en que se formula la solicitud, como también a la información necesitada, a fin de hacer posible el ejercicio del derecho, de un tratamiento de los datos.

4.2.2.2 Las causas de inadmisión de las solicitudes de acceso. La restricción del concepto de información pública establecido por el artículo 13

La Ley, consciente de los inconvenientes que podrían derivarse de un derecho tan ampliamente reconocido, ha establecido algunas causas de inadmisión de las solicitudes de acceso, cuya interpretación y aplicación pueden suponer una restricción importante del derecho reconocido en los

[540] Barrero Rodríguez, M.C. (2014). El derecho de acceso a la información: publicidad pasiva. En Guichot Reina, E. (Coord). *Transparencia, acceso a la información pública y buen gobierno. Estudio de la Ley 19/2013*, de 9 de diciembre. Madrid: Tecnos. p.204.

artículos 12 y 13. Se trata concretamente de las causas[541] referidas a: i) la información que esté en curso de elaboración o de publicación general; ii) la información de carácter auxiliar o de apoyo, como la contenidas en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas; y iii) la información para cuya divulgación sea necesaria una acción previa de reelaboración.

El artículo 18.1.b) exceptúa del derecho de acceso a una parte importante de la información en poder de las Administraciones al excluir aquellas solicitudes que se refieran a «información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas».

El contenido de esta excepción motivó el juicio negativo de E. GUICHOT, quien en su comparecencia ante la Comisión constitucional del Congreso denunciaba los riesgos que suponen los «informes internos» como causa de inadmisión, pues su aplicación «con carácter extensivo puede oscurecer buena parte de la actividad administrativa[542]». No existe en nuestro Derecho una definición de lo que debemos entender por información «auxiliar o de apoyo», como tampoco «los borradores, opiniones y los resúmenes», encuentran una definición precisa. A pesar de las críticas recibidas, la

---

[541] Artículo 18. Causas de inadmisión. 1. «Se inadmitirán a trámite, mediante resolución motivada, las solicitudes: a) Que se refieran a información que esté en curso de elaboración o de publicación general. b) Referidas a información que tenga carácter auxiliar o de apoyo como la contenida en notas, borradores, opiniones, resúmenes, comunicaciones e informes internos o entre órganos o entidades administrativas. c) Relativas a información para cuya divulgación sea necesaria una acción previa de reelaboración. d) Dirigidas a un órgano en cuyo poder no obre la información cuando se desconozca el competente. e) Que sean manifiestamente repetitivas o tengan un carácter abusivo no justificado con la finalidad de transparencia de esta Ley. 2. En el caso en que se inadmita la solicitud por concurrir la causa prevista en la letra d) del apartado anterior, el órgano que acuerde la inadmisión deberá indicar en la resolución el órgano que, a su juicio, es competente para conocer de la solicitud».

[542] Véase el Diario de sesiones del Congreso de los Diputados. X Legislatura, núm. 254, 12 de febrero de 2013, p. 20. Accesible en el siguiente link http://www.congreso.es/public_oficiales/L10/CONG/DS/CO/DSCD-10-CO-254.PDF

previsión fue aprobada en los mismos términos en los que figuraba en el Proyecto de Ley[543].

4.2.3 El procedimiento para el ejercicio del derecho

El apartado tercero del artículo 19 LTBG declara expresamente:

> *«Si la información solicitada pudiera afectar a derechos o intereses de terceros, debidamente identificados, se les concederá un plazo de quince días para que puedan realizar las alegaciones que estimen oportunas. El solicitante deberá ser informado de esta circunstancia, así como de la suspensión del plazo para dictar resolución hasta que se hayan recibido las alegaciones o haya transcurrido el plazo para su presentación».*

El sujeto obligado a facilitar la información deberá determinar, atendidas las características concretas de cada petición, su contenido y los posibles límites aplicables, quiénes son esas personas que, en su condición de terceros afectados, han de ser oídos en todo caso. Entre ellos, los titulares de datos personales especialmente protegidos, cuyo consentimiento expreso y por escrito es requisito obligado, como establece el apartado 1 del artículo 15[544] de la LTBG, para el acceso a la información. Este es, desde

---

[543] Este motivo de inadmisión ha merecido una valoración crítica de la mayor parte de los estudiosos de la norma. Así, y entre otros, Muñoz Soro J.F. y Bermejo Latre, J. L. (2014). La redefinición del ámbito objetivo de la transparencia y del derecho de acceso a la información del sector público. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*, Navarra: Thomson Reuters Aranzadi, pp. 232-233 o el propio Guichot Reina.E. (2014). Ejercicio del derecho de acceso a la información pública y régimen de impugnaciones. En Wences, I, Kólling, M. y Ragone, S. (Coords.) *La Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno. Una perspectiva académica*. *Cuadernos de Debate, 236, pp. 67-8.* Madrid: Centro de Estudios Constitucionales y Políticos.

[544] Artículo 15. Protección de datos personales. «1. Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso. Si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la

luego, el trámite natural y lógico para la manifestación de este consentimiento, lo que no obsta, dada la flexibilidad que caracteriza nuestro procedimiento, para que, si dispone de él, pueda presentarlo el propio solicitante al formular su petición de información[545].

El artículo 19.3 LTBG no prevé la posibilidad de que transcurra del plazo sin que el tercero haya formulado alegaciones, ante lo que procederá la aplicación de la regla prevista en el apartado tercero del artículo 82[546] de la Ley 39/2015 LPACAP, según la cual, se tendrá por realizado el trámite, lo que también ocurrirá en los supuestos en los que antes del vencimiento del plazo, esos terceros manifiesten su decisión de no efectuar alegaciones. Esta regla se excepcionará en los supuestos en que el tercero sea el titular de datos personales especialmente protegidos, pues en estos casos, se exigirá su consentimiento expreso y por escrito, conforme se establece en el primer apartado del artículo 15 LTBG.

En otro orden de cosas, el artículo 22[547] LTBG establece un conjunto de reglas al servicio de la garantía efectiva del derecho:

---

comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley».

[545] S Fernández Ramos, S. (2013). *El acceso a la información en el Proyecto de Ley de Transparencia, acceso a la información pública y buen gobierno, p. 274*. Zaragoza: IAAP, parece entender que en el caso de solicitudes de información que requieran el consentimiento expreso del afectado, «tal supuesto debe tratarse como de aportación de un documento necesario para tramitar la solicitud, de tal modo que si no se aporta con la solicitud el consentimiento el sujeto obligado deberá al solicitante para que subsane el defecto en plazo (artículo 71.1 LRJPAC), suspendiéndose el plazo para resolver por el tiempo que medie entre la notificación del requerimiento y su efectivo cumplimiento por el destinatario, o, en su defecto, el transcurso del plazo concedido (artículo 42.5.a) LRJPAC)».

[546] Artículo 82. Trámite de audiencia. «3. Si antes del vencimiento del plazo los interesados manifiestan su decisión de no efectuar alegaciones ni aportar nuevos documentos o justificaciones, se tendrá por realizado el trámite».

[547] Artículo 22. Formalización del acceso. «1. El acceso a la información se realizará preferentemente por vía electrónica, salvo cuando no sea posible o el solicitante haya señalado expresamente otro medio. Cuando no pueda darse el acceso en el momento de la notificación de la resolución deberá otorgarse, en cualquier caso, en un plazo no superior a diez días. 2. Si ha existido oposición de tercero, el acceso sólo tendrá lugar cuando, habiéndose concedido dicho acceso, haya transcurrido el plazo

– El acceso a la información «se realizará preferentemente por vía telemática, salvo cuando no sea posible o el solicitante haya señalado expresamente otro medio».
– En relación al plazo en que ha de producirse el acceso, «cuando no pueda darse el acceso en el momento de la notificación de la resolución deberá otorgarse, en cualquier caso, en un plazo no superior a diez días».
– En los supuestos en que haya existido oposición de un tercero, el acceso concedido solo tendrá lugar cuando «haya transcurrido el plazo para interponer recurso contencioso administrativo sin que se haya formalizado o haya sido resuelto confirmando el derecho a recibir la información».
– El acceso a la información es gratuito. «No obstante, la expedición de copias o la trasposición de la información a un formato diferente al original podrá dar lugar a la exigencia de exacciones en los términos previstos en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, o, en su caso, conforme a la normativa autonómica o local que resulte aplicable.

---

para interponer recurso contencioso administrativo sin que se haya formalizado o haya sido resuelto confirmando el derecho a recibir la información. 3. Si la información ya ha sido publicada, la resolución podrá limitarse a indicar al solicitante cómo puede acceder a ella. 4. El acceso a la información será gratuito. No obstante, la expedición de copias o la trasposición de la información a un formato diferente al original podrá dar lugar a la exigencia de exacciones en los términos previstos en la Ley 8/1989, de 13 de abril, de Tasas y Precios Públicos, o, en su caso, conforme a la normativa autonómica o local que resulte aplicable».

CAPÍTULO IVº: REUTILIZACIÓN

SUMARIO: 1 LA EVOLUCIÓN DESDE EL DERECHO DE ACCESO HASTA LA REUTILIZACIÓN DE LA DOCUMENTACIÓN PÚBLICA.–1.1 La regulación del derecho de acceso a la documentación pública.–1.2 El papel de la Unión Europea en la regulación de la reutilización de la información del sector público.–1.3 La evolución de las regulaciones sobre la información del sector público: del secreto a la comercialización de la información.–1.4 La aparición de nuevos protagonistas: el usuario y la intermediación de base tecnológica.–2 DIFERENCIAS ENTRE EL DERECHO DE ACCESO A LA INFORMACIÓN, LA PROTECCIÓN DE DATOS PERSONALES Y LA REUTILIZACIÓN DE LA INFORMACIÓN.–2.1 La relación entre la reutilización de la información y la protección de los datos personales.

1 LA EVOLUCIÓN DESDE EL DERECHO DE ACCESO HASTA LA REUTILIZACIÓN DE LA DOCUMENTACIÓN PÚBLICA.

4.3 La regulación del derecho de acceso a la documentación pública

Afirma SOLERNOU VIÑOLAS[548] que la libertad de información equivale al reconocimiento de una libertad individual de recibir información sobre las actuaciones políticas, decisiones o acuerdos, en este caso, de cualquier entidad pública. El derecho a obtener o deber de proveer información persigue la creación de la transparencia, principio que a su vez asegura la certeza en la acción de gobierno y salvaguarda de la arbitrariedad[549].

El acceso a la información legalmente establece el derecho público a saber, y a su vez, obliga al gobierno a informar al público. El principio de acceso a la información, en la mayoría de países, es un principio del cual se puede

---

[548] Solernou Viñolas, A. (2006). Los datos personales como límite a la reutilización de la información del sector público. En Cerrillo i Martínez, A. y Galán Galán, A. (Coord.): *La reutilización de la informació del sector público*. Granada: Comares. p 92.

[549] Así lo expone Kranenborg, H.y Voermans, W. (2005). *Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation*. Países Bajos: Europa Law Publishing, pág. 10 y ss.

decir que amplifica la democracia. Con él, se persigue la promoción de la participación de los ciudadanos en las decisiones de gobierno y en el proceso de elaboración de políticas públicas.

Es habitual calificar la sociedad actual como sociedad del conocimiento, destacando así el papel central que ha asumido la información, especialmente como consecuencia del desarrollo de las tecnologías de la información y del conocimiento. El uso de éstas por las administraciones públicas ha facilitado la difusión de la información del sector público y su conocimiento por los ciudadanos y las empresas.

La información bien suministrada puede ser un elemento que facilite la toma de decisiones y, desde este punto de vista, la transparencia puede estimular o alentar la eficiencia, promocionar la legitimidad y asistir en la fluida aplicación de las políticas públicas. En este sentido, la transparencia puede contribuir a legitimar las políticas y decisiones que toma el gobierno.

Conforme a lo dispuesto por el Supervisor Europeo de Protección de Datos[550], y de acuerdo con la sentencia del Tribunal de Primera Instancia de las Comunidades Europeas[551], no cabe argüir motivaciones concretas o particulares para requerir o solicitar acceso a la documentación de las instituciones de la Unión. La autoridad que decide el acceso a la documentación no está capacitada para exigir la justificación del motivo por

[550] Según el Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. Background Paper Series, 1. En https://edps.europa.eu/sites/edp/files/publication/05-07_bp_accesstodocuments_en.pdf, p. 9.

[551] Sentencia Tribunal de Primera Instancia Svenska Journalistförbundet v. Council, T-174/95, ECR (1998). P. II-2289. Establece que el objetivo de la Decisión del Consejo 93/731/CE, de 20 de diciembre de 1993, relativa al acceso del público a los documentos del Consejo**,** DOCE L-340 de 31/12/1993, es dar efectividad al principio de mayor acceso posible de los ciudadanos a la información desde la perspectiva de fortalecer el carácter democrático de las instituciones y la confianza del público en la administración. Expresamente se señala que no es necesario que el público alegue razones o fundamentos para el acceso a la documentación que solicitan.

el cual alguien solicita el acceso, no está habilitada para ponderar la importancia del acceso respeto la persona que lo solicita[552].

Aunque la Unión Europea no tiene competencias para regular expresamente el derecho de acceso en el marco de la libertad de información, su regulación propia, al ser aplicable a todos los documentos que obran en poder de las instituciones comunitarias, puede incluir mucha documentación elaborada o desarrollada por los Estados miembros que ha sido presentada o tiene como destino las instituciones de la Unión. Así, se puede dar la contradicción que un mismo documento a nivel nacional no sea de libre acceso para los particulares y en cambio sí tenga esta condición ante las instituciones europeas. Se proclama la necesidad de armonizar las regulaciones existentes a nivel nacional y comunitario en esta materia, en tanto la información no reside de forma estanca en un único destino, sino que fluye entre las diversas instituciones y organismos nacionales y comunitarios de forma constante.

La regulación del acceso a la documentación administrativa en la Constitución Española se sitúa en el marco de los principios que rigen la actuación administrativa. La regulación existente actualmente del derecho

---

[552] Así, el artículo 2 del Reglamento 1049/2001, de 30 de mayo de 2001, en relación a los beneficiarios y el ámbito de aplicación, declara expresamente que «1. Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tiene derecho a acceder a los documentos de las instituciones, con arreglo a los principios, condiciones y límites que se definen en el presente Reglamento. 2. Con arreglo a los mismos principios, condiciones y límites, las instituciones podrán conceder el acceso a los documentos a toda persona física o jurídica que no resida ni tenga su domicilio social en un Estado miembro. 3. El presente Reglamento será de aplicación a todos los documentos que obren en poder de una institución; es decir, los documentos por ella elaborados o recibidos y que estén en su posesión, en todos los ámbitos de actividad de la Unión Europea. 4. Sin perjuicio de lo dispuesto en los artículos 4 y 9, los documentos serán accesibles al público, bien previa solicitud por escrito, o bien directamente en forma electrónica o a través de un registro. En particular, de conformidad con el artículo 12, se facilitará el acceso directo a los documentos elaborados o recibidos en el marco de un procedimiento legislativo. 5. Se aplicará a los documentos sensibles, tal como se definen en el apartado 1 del artículo 9, el tratamiento especial previsto en el mismo artículo. 6. El presente Reglamento se entenderá sin perjuicio de los derechos de acceso del público a los documentos que obren en poder de las instituciones como consecuencia de instrumentos de Derecho internacional o de actos de las instituciones que apliquen tales instrumentos.

de acceso[553], se dicta de conformidad con lo que establece el artículo 105. b) de la CE.

4.4 El papel de la Unión Europea en la regulación de la reutilización de la información del sector público

La nuestra, se puede definir como una sociedad caracterizada por la creciente tendencia a reciclar, ya sea por motivos medioambientales o estrictamente económicos, unos recursos habitualmente escasos. Entre estos, se encuentra la información que tiene un valor económico nada despreciable. Las administraciones públicas pueden reutilizar la información que generan, ya sea comercializándola directamente, o facilitando que la reutilización y explotación comercial se realice a través de terceros. La información del sector público puesta a disposición por parte de la administración pública, tiene un potencial económico importante.

Esta situación ha llevado a que los poderes públicos hayan ido adoptando diferentes normas, que más allá de regular el acceso de los ciudadanos a la información administrativa o su difusión por parte de las propias administraciones públicas, regulen la reutilización y la comercialización de la información por parte del sector privado.

La Unión Europea ha ido adoptando diferentes documentos y aprobando diversas normas en relación a la información tanto de las instituciones comunitarias como de las administraciones públicas de los Estados miembros. Todos estos documentos y normas pueden agruparse a efectos expositivos en tres grupos en función del objetivo principal que persiguen.

---

[553] Véase la letra d) del artículo 13 en relación a los derechos de las personas en sus relaciones con las Administraciones Públicas, de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. «Quienes de conformidad con el artículo 3, tienen capacidad de obrar ante las Administraciones Públicas, son titulares, en sus relaciones con ellas, de los siguientes derechos: […] d) Al acceso a la información pública, archivos y registros, de acuerdo con lo previsto en la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico».

4.4.1 La creación del mercado de la información del sector público en Europa

La primera iniciativa europea relativa a la comercialización de la información del sector público la encontramos en las Directrices para mejorar la sinergia entre los sectores público y privado en el mercado de la información[554]. Las Directrices perseguían convencer al sector público de que facilitase el uso por el sector privado de las informaciones que ostenta.

La Comisión Europea retomó su interés por la reutilización de la información del sector público en 1996, al redactar el Libro Verde sobre la información

---

[554] Expresamente se reconocía en ellas «Los gobiernos y los organismos del sector público recogen gran cantidad de datos e información, como parte de su tarea habitual, que podrían ponerse a disposición del sector privado para la elaboración y comercialización de servicios electrónicos de bases de datos. El sector privado se halla en una buena situación para combinar la información procedente de una diversidad de fuentes estatales, y su principal función consiste en producir y distribuir productos de la información destinados a cubrir las necesidades del mercado. Para desarrollar y fortalecer la industria de la información es necesaria la iniciativa decidida por parte de los gobiernos, con el fin de fomentar la utilización y la explotación de la información y los datos del sector público. De las Directrices recogidas, destacamos las siguientes: i) Las administraciones públicas recogen datos básicos e información de un modo regular y sistemático en el desempeño de sus funciones estatales. Esta recogida de datos es de gran valor no solo para los gobiernos y su mayor disponibilidad sería beneficiosa tanto para el sector público como para la industria privada. Las organizaciones públicas, siempre que resulte practicable y su acceso no se halle restringido por motivos de protección legítima de intereses públicos o privados, deberían permitir la utilización de esta información básica por parte del sector privado así como su explotación por la industria de la información a través de servicios electrónicos de información; ii) Los Estados miembros habrán de recopilar y publicar directrices por las que se definan las condiciones de cesión, uso y explotación de datos e información del sector público; v) Cuando se distribuyan datos o información del sector público para su explotación por parte del sector privado, no deben hacerse restricciones relativas al tipo de cliente o los territorios en los que se hagan disponibles los servicios resultantes; vi) Los contratos o cualquier otro acuerdo con proveedores o servicios centrales de bases de datos del sector privado no deberían conceder derechos exclusivos si con ello se produjeran distorsiones de la competencia. Si, por razones como la penetración de un nuevo mercado o el suministro de un servicio de interés público, se considerara necesario conceder un derecho exclusivo, debería ser sometido a una revisión periódica». «Directrices para mejorar la sinergia entre los sectores público y privado en el mercado de la información». Oficina de Publicaciones de las Comunidades Europeas. Bruselas. 1989. Están accesibles en el siguiente link http://bookshop.europa.eu/es/directrices-para-mejorar-la-sinergia-entre-los-sectores-p-blico-y-privado-en-el-mercado-de-la-informaci-n-pbCD5488126/downloads/CD-54-88-126-ES-C/CD5488126ESC_001.pdf;pgid=GSPefJMEtXBSR0dT6jbGakZD0000cuYPOj8L;sid=38hvDx3puUlvCEV3NvHxqH_M2Btp3L8qo5g=?FileName=CD5488126ESC_001.pdf&SKU=CD5488126ESC_PDF&CatalogueNumber=CD-54-88-126-ES-C

del sector público[555]. En éste, se indica que «una buena disponibilidad de la información pública es un requisito previo indispensable para la

[555] Al analizar la relevancia de la información que ostentan las administraciones u otras entidades públicas, el Libro Verde lo hizo desde una doble perspectiva haciendo hincapié en su relevancia para corregir el déficit democrático de la Unión, como mecanismo de transparencia pero también su relevancia en el mercado, como recurso para incentivar el desarrollo económico y como instrumento para facilitar el ejercicio de las libertades de las personas, en concreto la libertad de residencia y la libre circulación. En relación con la política de fijación de precios, el doble objetivo de una política de información del sector público que comprenda acceso y comercialización, requiere una política de fijación de precios que tenga en cuenta los diferentes intereses en juego: que el acceso sea asequible para todos para garantizar la participación de todas las personas, cuál es el potencial de la comercialización y que ésta sea en competencia leal con el mercado. Debe tenerse en cuenta que la información del sector público se elabora y produce a costa del contribuyente y se plantea si los organismos públicos tienen derecho a cobrar por la información que ha sido desarrollada gracias al esfuerzo de todos los ciudadanos. Por contrapartida, se aduce que no todo el conjunto de la población debe soportar los costes de la reutilización, sino únicamente aquellos que estén interesados, los cuales deberán pagar una contraprestación. La política de precios, los destinatarios de la información y la inmediatez en el suministro de la misma, tienen una gran relevancia en materia de competencia y de libre mercado. Un aspecto a tener en consideración es la responsabilidad de la administración respecto a la información difundida que exige abordar la valoración de aquellos supuestos de información errónea, incompleta u omitida y los daños que puedan derivar de ella. Por otro lado, el Libro Verde califica las excepciones al derecho de acceso a la información del sector público, interpretando acceso en términos generales, como toda revelación a terceras partes de los documentos de los que disponen las administraciones públicas ya sea en un contexto nacional o comunitario, en diferentes categorías. En primer lugar, señala las excepciones en interés del Estado, basadas en motivos de seguridad nacional, orden público, intereses económicos, relaciones internacionales, procedimientos legislativos, etc., asuntos en general de competencia exclusiva del Estado. Otras excepciones residen en la protección de los intereses de terceros, como son la protección de la intimidad, la propiedad intelectual, los secretos comerciales o industriales o los procedimientos judiciales que pueden afectar a las partes. En tercer lugar, existen aquellas excepciones que se dirigen a proteger el proceso decisorio, ya sea la información de naturaleza preliminar o sea la información interna. Ahondando en una de las excepciones manifestadas, otro aspecto a tener en cuenta está relacionado con la intimidad y la protección de los datos personales. La información comercialmente interesante del sector público tiene, en muchos casos, naturaleza personal o hace referencias directas o indirectas a personas físicas. La industria tiene notable interés en utilizar esta información con fines meramente comerciales o para la investigación del sector. En todo caso, debe sopesarse el derecho a la información de los ciudadanos y las empresas con el derecho del particular a la intimidad y a la protección de sus datos personales. El Libro Verde señaló en el punto 112 que «la Directiva 95/46/CE establece normas vinculantes tanto para el sector público como para el privado y logra el necesario equilibrio entre el principio de acceso a la información del sector público y la protección de los datos personales. Es de obligado cumplimiento en los casos de datos personales en manos del sector público». Todas las normas nacionales de acceso deben tener presente la necesidad de este equilibrio, que será necesario tanto en la ponderación de protección de datos e intimidad versus el acceso en el marco de la libertad de información como *versus* la reutilización de la información, sea con fines comerciales o no. Así, el punto 113 del mismo establece expresamente que son los entes públicos competentes los que deberán

competitividad de la industria europea», siendo una oportunidad para el crecimiento económico y el empleo. Señala que la falta de información y la opacidad implican elevados costes para aquellas empresas privadas que requieren datos actualizados, y a su vez, una información suministrada de forma rápida y veraz beneficia a particulares y compañías que desarrollan actuaciones en diferentes Estados miembros. Éste llega a afirmar que en la economía y sociedad actual, «el hecho de que los ciudadanos y consumidores de la UE no puedan utilizar de la mejor manera la información pública disponible en otros Estados miembros de la UE es algo anacrónico». Perseguía recoger la opinión[556] de los actores europeos a fin de poder avanzar en la elaboración de una norma sobre reutilización de la información del sector público en Europa, ya que era difícil encontrar en Europa normas sobre las condiciones de explotación de la información del sector público por parte del sector privado.

Sin embargo, hubo que esperar al año 2003 para aprobar la Directiva 2003/98/CE[557]. La información del sector público se califica como un recurso

---

garantizar el equilibrio entre la necesidad de un acceso libre para fines comerciales u otros y el respeto de la intimidad, teniendo en cuenta los principios establecidos en la Directiva 95/46/CE. Finalmente se señalan aquellas excepciones que lo son para evitar costes o cargas de trabajo desmesuradas en las administraciones afectadas, de modo que se puede limitar el acceso en aquellos supuestos en que la información a divulgar requiere un tratamiento adicional, cuando hay un exceso de solicitudes o cuando la información ya se encuentra publicada por otros medios. Surgen algunas dudas en relación a si el derecho se extiende a un derecho a acceder a los datos en bruto, a la información intermedia o únicamente a aquellos datos finales que han sido definitivamente elaborados. El tema plantea la dificultad de decidir si los datos en bruto pueden ser poco relevantes para el público en el formato en el que se encuentran y si puede generar esfuerzos desproporcionados la preparación o adaptación de esta información para su divulgación pública. «La información del sector público: un recurso clave para Europa. Libro verde sobre la información del sector público en la sociedad de la información». COM(1998) 585. Accesible en el link http://cordis.europa.eu/pub/econtent/docs/gp_es.pdf

556 Expresamente reconocía «la necesidad de llevar a cabo un debate concertado a escala europea es ahora más clara y urgente que nunca. El objetivo del presente Libro verde es emprender una amplia consulta pública entre todos los operadores afectados con miras a estudiar los principales problemas y a suscitar un debate político a escala europea».

557 Directiva 2003/98/Ce del Parlamento Europeo y del Consejo de 17 de noviembre de 2003 relativa a la reutilización de la información del sector público. DOUE L345, 31.12.2003, modificada en la actualidad por la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013. DOUE L175 de 27.6.2013. La Directiva constituye el punto de llegada de los trabajos realizados por la Unión Europea respecto a los contenidos del sector público y su comercialización en el mercado

esencial, ya sea como fuente de conocimiento o para generar desarrollo económico. El sector público surge como un gran productor de contenidos, de elaboración propia o externa, que pueden suplir las necesidades de la red y de la sociedad en general, y esta Directiva pretende establecer las pautas necesarias para la puesta a disposición de esta información y para la definición de los usos. La reutilización es definida por el artículo 2.4 de la

---

interior. Sin embargo, no incide en la regulación del derecho de acceso a la información administrativa. Destaca CERRILLO I MARTÍNEZ [Cerrillo i Martínez, A. (2006). La información del sector público: del acceso a la reutilización. En Cerrillo Martínez, A. y Galán Galán, A. (Coord.), *La reutilización de la información del sector público*. Granada: Comares. p 17] que los objetivos de la Directiva: i) Facilitar la creación de productos y servicios de información basados en documentos del sector público que cubran la totalidad de la Comunidad; ii) Reforzar la eficacia del uso transfronterizo de documentos del sector público por las empresas privadas para que ofrezcan productos y servicios de información de valor añadido; y iii) Limitar el falseamiento de la competencia en el mercado comunitario. Esta Directiva persigue: a) armonizar las normas y prácticas del sector público con el fin de contribuir a la creación del mercado interior y de un sistema que impida el falseamiento de la competencia en dicho mercado; b) establecer un marco general para las condiciones de la reutilización de la información del sector público. Estas condiciones deben ser equitativas, proporcionadas y no discriminatorias; y c) armonizar las condiciones mínimas que deben permitir la reutilización de la información teniendo en cuenta las divergencias existentes en las diferentes tradiciones jurídicas de los Estados miembros. De esta manera, se pretenden superar las barreras que habían limitado el crecimiento del mercado europeo de los contenidos, haciéndolo competitivo frente al norteamericano. Así, uno de los principales objetivos del establecimiento de un mercado interior es la creación de unas condiciones que favorezcan el desarrollo de servicios que abarquen toda la Comunidad. De acuerdo con el Considerando 5 de la Directiva 2003/98/CE, «la información del sector público constituye una materia prima importante para diferentes productos y servicios de contenidos digitales por lo que se deben establecer las normas que permitan y faciliten aprovechar su potencial y contribuir al crecimiento económico y a la creación de empleo». Sin embargo, la Directiva está redactada en términos muy amplios, y no se deriva de la misma un único régimen jurídico de la reutilización y la comercialización de la información del sector público para toda la Unión europea. Así se especifica en su Considerando 9 al establecer que «la presente Directiva no contiene la obligación de autorizar la reutilización de autorizar la reutilización de documentos. La decisión de autorizar o no la reutilización corresponderá a los Estados miembros o al organismo del sector público que corresponda». Esta Directiva exige que las condiciones de reutilización no sean discriminatorias para tipos comparables de reutilización, lo que no impide el intercambio gratuito de información entre organismos del sector público, cuando estos desarrollen misiones de servicio público, mientras que otras partes deban abonar una tarifa por la reutilización de los mismos documentos. Por tanto, se legitima por parte de la misma una política de tarifas diferenciada para la reutilización comercial y no comercial. Diferenciación que pone de manifiesto la relevancia que puede tener la finalidad del destino de la información. A pesar de que el fundamento de la actividad de difusión y de comercialización de la información del sector público es diferente, la transposición de la directiva debe favorecer un cambio de cultura respecto a la comercialización de la información del sector público en las administraciones públicas, y debe potenciar el valor de esta información.

Directiva 2003/98/CE como «el uso de documentos que obran en poder de organismos del sector público por parte personas físicas o jurídicas, con fines comerciales o no comerciales, distintos del propósito inicial que tenían esos documentos en la misión de servicio público para la que se produjeron». Sin embargo, el intercambio de documentos entre organismos del sector público en el marco de sus actividades de servicio público, no se considerará reutilización, pues ésta requiere que el uso de destino de la información sea ajeno al ejercicio de las funciones públicas que ocasionaron su elaboración.

Afirma CERRILLO i MARTÍNEZ[558] que, hasta la aprobación de esta Directiva, en Europa no existían unas normas generales que establecieran las condiciones de la explotación de la información del sector público por parte del sector privado[559], ni tampoco unos principios claros y coherentes, más allá de la regulación en sectores como el de la información cartográfica o estadística. Todo ello colocaba a la industria europea en desventaja competitiva respecto a la de Estados Unidos de América[560].

---

[558] Cerrillo i Martínez, A. (2006). La información del sector público: del acceso a la reutilización. En Cerrillo Martínez, A. y Galán Galán, A. (Coord.), *La reutilización de la información del sector público*. Granada: Comares. p 10.

[559] Expresamente los apartados 42 y 43 del Libro Verde sobre la información del sector público en la sociedad de la información afirman que es difícil encontrar en Europa normas sobre las condiciones de explotación de la información del sector público por parte del sector privado. A pesar de algunas buenas iniciativas, no existe un conjunto de principios claro y coherente para Europa. Esta falta de principios claros y coherentes hace que la industria europea se halle en una desventaja competitiva frente a la de Estados Unidos.

[560] Ramos Simón, F. (2003). La reutilización de la información del sector público. Aproximación del contenido de la propuesta de directiva 2002. *Revista General de Información y Comunicación, 13, núm. 2*, pág. 69. Viene a afirmar que en Estados Unidos de América la «Free information Act» logró grandes estímulos para que el sector privado comercializara la información del sector público. Es preciso hacer mención a la «Electronic Freedom of Information Act Ammendments», que complementa y modifica otras leyes, como son la Ley de reducción de trámites burocráticos y la Ley de trasparencia del Gobierno, incluida la «Freedom of Information Act». El objetivo de esta reforma fue adaptar la regulación del acceso a la información a los canales de difusión telemática. Ambas normas, además de regular el acceso a la información del sector público, inciden en la reutilización y la comercialización de la información. El propósito básico de la ley es asegurar una ciudadanía informada, vital para el funcionamiento de una sociedad democrática, necesario frente a la corrupción

La reutilización no tiene un enfoque únicamente comercial, sino que persigue también el incremento de la documentación al alcance de los ciudadanos como fuente de conocimiento. Se pretende que la información del sector público deje de estar únicamente a disposición de las administraciones públicas y pueda ser aprovechada por los particulares o por empresas privadas, sea gratuitamente o previa remuneración, sea para un uso particular o para su explotación comercial.

La evolución de una administración burocrática a la administración en red[561] supone reconocer un papel esencial a la información y que el acceso a la

---

y sostén del control de los políticos por los gobernados. Esta ley prevé que cualquier persona pueda solicitar información, por cualquier razón. No es necesario justificar la petición.

[561] Cerrillo i Martínez declara que «podemos establecer tres estadios en el proceso evolutivo de las relaciones entre administraciones públicas y los ciudadanos en función del papel más o menos activo conferido a estos últimos: la administración burocrática, la administración recepticia y la administración en red. I) Administración burocrática y secreto. El modelo de administración burocrática consiste en una organización basada en un conjunto de funciones formales establecidas mediante reglas legales, racionales, escritas y exhaustivas, basado en los principios de legalidad y jerarquía. La organización burocrática respondía a un tipo de dominación legal-racional, cuya legitimidad se basaba en la creencia en la legalidad de los reglamentos promulgados y del derecho, para el detentador del poder, de dar órdenes. Ello llevaba a la necesidad de defender una administración pública cerrada, una administración pública que no tenía la necesidad de escuchar a los ciudadanos, ni tampoco convencerles de sus acciones ni, por tanto, informarles de sus acciones. Por lo que una de las características de la administración burocrática era el secreto y el distanciamiento que, en general, existía entre la Administración y los ciudadanos. El modelo de administración burocrática va evolucionando y es necesario establecer nuevos mecanismos que permitan legitimar su actuación. A su vez, también se incrementan las reivindicaciones sociales en favor de la plena incorporación del principio democrático en la actuación pública, lo que supondrá la adopción de nuevos principios rectores de la actuación administrativa. En el momento de la aprobación de la Constitución en 1978, se dan las condiciones idóneas para afianzar estos mecanismos y establecer los principios jurídicos sobre los que se deben sustentar. Y de hecho, como sostiene MESTRE DELGADO, la amplitud con que se configura el derecho de acceso en el texto constitucional permite sostener el principio de transparencia en la actuación administrativa. El principio de transparencia que prevé la Constitución está plenamente relacionado con otros principios básicos del sistema democrático, como el de eficacia, seguridad jurídica y de legalidad. Además, otros preceptos constitucionales, como el previsto en el art. 20 al reconocer y garantizar el derecho a la información, tienen incidencia en esta materia. Con posterioridad a la Constitución, algunas normas, como la Ley de Bases del Régimen Local o la Ley de Patrimonio Histórico Español, hacen referencia al acceso a la información administrativa, aunque sin desarrollar claramente su régimen jurídico. Ello no sucede hasta la aprobación de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común; II) Administración receptiva y comunicación pública. La crisis del modelo burocrático de Administración pública ha llevado

consigo la aparición de nuevos modelos con el objetivo de reemplazarlo y superar las rigideces que le eran inherentes. La receptividad, en un principio, y la orientación al cliente y la gestión de la calidad, posteriormente, han sido algunas de las respuestas del sistema a esta crisis del modelo durante los años ochenta. Como ha señalado VILLORIA, el concepto de administración receptiva se caracteriza, sin negar el modelo de legitimación racional-legal, por el desarrollo de la diversidad, complejidad y dinámica constante; los valores del individuo cliente y el culto al mercado, la privatización y la canonización de la mano invisible. Pero además, la incorporación del concepto de administración receptiva supone que la Administración dará respuestas rápidas y flexibles a las demandas de los ciudadanos, y que imprimirá calidad a los servicios que preste. El proceso de modernización de las administraciones públicas ha supuesto, entre otros extremos, una variación de la conceptualización de los administrados que han pasado a considerarse clientes de los servicios administrativos, lo que ha significado situarles en el centro de la actividad administrativa. Así, los ciudadanos, vistos como clientes, gozan en la actualidad de un estatus revitalizado frente a las administraciones públicas, lo que les confiere un haz de derechos y facultades para desarrollar sus necesidades, entre los que se encuentra el de obtener información de la Administración. La LRJPAC, superando la tradicional nominación de administrados, reconoce en su art. 35 un conjunto de derechos de los ciudadanos en sus relaciones con las administraciones públicas. Del conjunto de derechos de los ciudadanos previstos en el art. 35 LRJPAC, hay cuatro que están referidos a la información administrativa de los ciudadanos: i) Derecho a conocer el estado de la tramitación de los procedimientos; ii) Derecho a identificar a las autoridades y al personal al servicio de las administraciones públicas; iii) Derecho a obtener información acerca de los requisitos jurídicos o técnicos; y iv) Derecho a acceder a los archivos y registros administrativos. Sin entrar con detalle a valorar la extensión de estos derechos, se puede observar que nos encontramos ante auténticos derechos subjetivos. El reconocimiento de estos derechos a obtener información administrativa implica, por un lado, la obligación particular de facilitar información administrativa ante una solicitud en este sentido por parte de un ciudadano y, por otro, el establecimiento de un deber genérico de organizar los servicios competentes para facilitar la información a los ciudadanos. Por un lado, está la información administrativa general (información sobre los requisitos jurídicos o técnicos con relación a proyectos, actuaciones o solicitudes e información sobre documentos que se encuentren en archivos y registros). Para acceder a esta información, no se requiere ninguna legitimación especial. Cualquier ciudadano puede acceder a ella. Por otro lado, para poder acceder a la información administrativa particular que se refiere a procedimientos concretos y específicos, se requiere tener la condición de interesado. En definitiva, la LRJPAC ha supuesto una consolidación del ciudadano frente a la Administración pública con relación a la actividad informativa. Ahora bien, surge como necesario el establecimiento de mecanismos idóneos para que los ciudadanos puedan ejercer los derechos previstos. Posteriormente a la aprobación de la LRJPAC, la regulación de la actividad informativa se ha visto ampliada, por un lado, con la aprobación de normativas sectoriales que inciden en esta actividad (sanidad, educación, medio ambiente, por citar unos ejemplos) y, por otro lado, con la aprobación de las normas que han establecido la infraestructura necesaria para el desarrollo de esta función. El Real Decreto 208/1996 prevé diferentes mecanismos mediante los cuales los ciudadanos podrán acceder a la información haciéndose una especial mención a los mecanismos de información presencial, como las oficinas de información y atención a los ciudadanos. Sin embargo, esta regulación no hace referencia ni a la posición jurídica del ciudadano respecto a la actividad informativa ni a las características ni condiciones en las que las administraciones públicas deben desarrollar la actividad informativa; y III) Administración en red y transparencia. La administración en red describe un modelo de administración pública propio de las sociedades pluralistas, complejas

misma sea ágil y eficiente por parte de los particulares, sean personas físicas individuales o empresas que desarrollan su actividad en el mercado. Esta información debe ser de calidad, objetiva, de fácil entendimiento y completa.

4.4.2 El acceso a la información del sector público

En segundo lugar, la preocupación de la Unión Europea en relación a la información del sector público, se ha centrado en regular el acceso de los ciudadanos a la información pública. Desde esta perspectiva, la Unión

---

e interdependientes, que se basa en la colaboración entre administración y ciudadanos, y no sólo en la reivindicación: supone el paso de un concepto de administración de tipo jerárquico a uno de administración en forma de red, en el que se dan múltiples relaciones entre los diferentes nodos o actores representantes, todos ellos de intereses que deben integrarse en la composición del interés general debido a la interdependencia que existe entre sí. Con la administración en red se pretende superar el modelo tradicional de administración basado en el binomio autoridad-libertad en el que la Administración usa el poder administrativo como principal instrumento de intervención, e ir hacia un modelo basado no tanto en el ejercicio del poder, como en que se desarrollen de manera imparcial y eficiente las funciones públicas de interés general. El modelo propuesto supone el reconocimiento de la existencia de redes de relaciones entre sujetos autónomos que actúan dentro de ella siguiendo una lógica de colaboración. De estas relaciones resultan beneficios o ventajas para todos los sujetos participantes. Todos ellos, aunque sea en medidas diversas, son portadores de recursos que aportan al interior de la red, combinándose e intercambiándose con los aportados por el resto de sujetos de manera que cada uno puede ver satisfechas sus propias necesidades. La extensión de las redes es un proceso generalizado en las sociedades actuales. CASTELLS afirma al respecto que «las redes configuran nuestras sociedades, y los procesos de producción, experiencias, poder y cultura están ampliamente determinados por la lógica de estas redes». La administración en red tiene importantes consecuencias en la manera de funcionar de los poderes públicos al suponer que numerosos actores (no sólo públicos) están implicados en la formulación e implementación de las políticas. Para que la pluralidad de actores pueda participar en las deliberaciones y toma de decisiones que se desarrollan en las redes, es necesario que existan niveles adecuados de información y de transparencia. La gobernanza de la administración en red tiene como requisito previo y necesario la información y la transparencia a fin de garantizar y facilitar la participación de todos los actores implicados. Es necesario que todos los actores que intervienen en las redes puedan participar de forma informada. Ello requiere que tengan a su disposición la información y el conocimiento adecuado y que pongan a disposición del resto de actores la información y el conocimiento de que disponen. La información es un recurso imprescindible en los procesos de toma de decisiones. Los actores estratégicos que participen en ellos tendrán la información como un elemento sobre el que podrán articular su intervención en las redes. La información se convierte en un recurso de poder que cada actor establecerá sobre la base del resto de los recursos de que disponga y que marcará sus estrategias en el marco de las redes. En esta tarea pueden ser de gran utilidad las tecnologías de la información y la comunicación». Cerrillo i Martínez, A. (2005). E-información: hacia una nueva regulación del acceso a la información. *Revista Internet, Deret i Política pp 2-6*. Recuperado de http://www.uoc.edu/idp/1/dt/esp/cerrillo.pdf

Europea ha perseguido incrementar la transparencia de la Unión Europea, la proximidad a los ciudadanos y, al fin y al cabo, la legitimidad democrática de las instituciones comunitarias.

Desde que en el Tratado de Maastricht se recogió una declaración para establecer el principio de transparencia de la Unión Europea, se han ido sucediendo declaraciones políticas, y normas que han desarrollado dicho principio, a través del derecho de acceso a los documentos administrativos.

Por otro lado, respecto al acceso a la información de las instituciones comunitarias mediante la aprobación de un conjunto de normas por parte de diversas instituciones que posteriormente se ha constitucionalizado en los diversos tratados[562]. Estas normas constituyeron un paso importante en el reconocimiento del principio de transparencia administrativa y del derecho de acceso a la información administrativa en Europa[563]. Actualmente, es el Reglamento (CE) 1049/2001 el que consolida las iniciativas ya adoptadas por las instituciones con vistas a aumentar la transparencia del proceso de toma de decisiones.

4.4.3 El fomento de los contenidos digitales

La Unión Europea ha ido adoptando diversas políticas públicas relativas a la sociedad de la información y los contenidos e Internet que han incidido en el ámbito de la reutilización de la información del sector público. Las preocupaciones de las instituciones comunitarias se han centrado en tres aspectos principales: la creación de contenidos digitales públicos, la

---

[562] Véanse al respecto los artículos 255 del Tratado de Ámsterdam, 41 y 42 de la Carta de los Derechos Fundamentales de la Unión Europea y I-50 del Proyecto de tratado por el que se establece una Constitución para Europa.

[563] Decisión 93/731/Ce del Consejo, de 20 de diciembre de 1993, relativa al acceso del público los documentos del Consejo, la Decisión 94/90/CECA, CE, Euratom del Parlamento Europeo, de 10 de julio de 1997, relativa al acceso del público a los documentos del Parlamento Europeo y las normas de confidencialidad de los documentos de Schengen. Véase un análisis detallado de estas normas en Cerrillo i Martínez, A. (1998). *La transparencia administrativa: Unión Europea y medio ambiente*. Valencia: Tirant lo Blanch.

utilización de las lenguas europeas y el impulso de las plataformas multicanales.

Como punto de partida, se puede señalar el programa INFA 2000[564], con el objetivo de hacer que los recursos de información en poder del sector público estuvieran más fácilmente disponibles para su comercialización en servicios europeos de contenidos multimedia.

El Plan de acción eEuropa 2002[565] estableció los objetivos para introducir plenamente a Europa en la era digital y propuso la creación de un marco comunitario para la explotación comercial de la información del sector público. Se destaca el potencial de crecimiento del sector, y se pone de relieve que existen actividades desarrolladas por organismos públicos que pueden ser susceptibles de incorporar al mercado información (por ejemplo, información comercial y financiera, información jurídica, información científica y técnica o información geográfica). Se apuntó expresamente que «la incertidumbre sobre las condiciones de utilización de los datos impide que las empresas se lancen a la explotación transfronteriza de la información del sector público y puede disuadir especialmente a las PYME, que no pueden permitirse inversiones improductivas importantes».

4.4.4 La relevancia actual de la información del sector público

La sociedad de la información se identifica con el estadio de la sociedad postindustrial en el que la información es un elemento del entorno, de modificación de las condiciones de vida, de dirección de la innovación y del

---

564 96/339/CE: Decisión del Consejo, de 20 de mayo de 1996, por la que se adopta un Programa plurianual de la Comunidad para fomentar el desarrollo de la industria europea de los contenidos multimedios y la utilización de éstos en la naciente sociedad de la información (INFA 2000) DOCE L 129 de 30.5.1996. el texto completo se encuentra accesible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31996D0339&qid=1496425689773&from=ES

565 Comunicación de la Comisión al Consejo, el Parlamento Europeo, el Comité Económico y Social y el Comité de las Regiones. La eEUROPE 2002: creación de un marco comunitario para la explotación de la información del sector público, de 23.10.2001 COM (2001) 607 final. Texto accesible en http://ec.europa.eu/transparency/regdoc/rep/1/2001/ES/1-2001-607-ES-F1-1.Pdf

cambio social[566]. La información y el conocimiento que genera tienen un fuerte impacto en la vida de todos los europeos y puede convertirse en un motor de crecimiento, competitividad y empleo, al tiempo que mejora la calidad de vida de los ciudadanos. Las tecnologías de la información y la comunicación han potenciado este papel de la información como motor de desarrollo. En particular, se puede apuntar que las tecnologías de la información y la comunicación están ampliando enormemente la información en poder de los ciudadanos y están diversificando de forma importante, tanto cuantitativa como, especialmente, cualitativamente, los mecanismos de gestión y transmisión de la información lo que está incidiendo de manera importante en los diferentes usos que se dan a la información del sector público.

Las administraciones públicas crean, recopilan, tratan, almacenan, distribuyen y difunden grandes cantidades de información en el ejercicio de sus funciones. La información del sector público desarrolla un papel relevante en el ejercicio de los derechos y en la realización del quehacer diario no sólo de las administraciones públicas sino también de los ciudadanos y de las empresas [567]. El aprovechamiento de los contenidos genera riqueza y conocimiento y, a su vez, la elaboración y la producción de éstos es también una fuente rápida de creación de empleo.

Para los ciudadanos, el acceso a la información del sector público le permite ejercer sus derechos, participar en la toma de decisiones públicas y controlar la actividad de la información exigiendo, en su caso, la oportuna rendición de cuentas. La información del sector público juega un papel fundamental en el desarrollo de la democracia al facilitar a los ciudadanos la base necesaria para poder participar en la toma de decisiones públicas.

---

[566] Castells, M. (1996). La era de la información. Volumen I. La sociedad red. Madrid: Alianza.

[567] Cerrillo i Martínez, A. (2000). Régimen jurídico de la información administrativa. En Tornos Mas, J. y Galán Galán, A. *La comunicación pública. La información administrativa al ciudadano*. Madrid: Marcial Pons, págs. 213 y sigs. En la misma línea, Comisión Europea (2001) *eEUROPE 2002 op. cit.*

Para las empresas, la información del sector público le permite llevar a cabo su actividad, así como definir sus estrategias y mejorar su competitividad. Pero además, para las empresas de contenidos, también presenta un considerable potencial económico ya que es la base esencial para muchos productos de información digital, siendo una materia prima para nuevos servicios. Desde esta perspectiva, la información del sector público y la industria de los contenidos son generadores de riqueza y de empleo.

La economía digital basada en el conocimiento tiene un fuerte impacto en la vida de todos los europeos y puede convertirse en un motor de crecimiento, competitividad y empleo, al tiempo que mejora la calidad de vida de los ciudadanos. Un mejor acceso y utilización de esta información constituiría un valioso activo para los ciudadanos, las empresas y las administraciones. Los ciudadanos y las empresas podrán extraer un enorme beneficio de la disponibilidad de información del sector público a través de Internet. Con ello se facilitará su comunicación con las administraciones públicas y se les ofrecerá una posibilidad de incrementar su participación en el proceso democrático. La información del sector público es un activo económico y una mercancía en potencia. Estos usos se ven reforzados en la sociedad de la información debido a que los constes de difusión y de reproducción se han reducido de forma muy importante. Las tecnologías de la información y la comunicación facilitan la recolección de la información, así como su presentación, distribución, difusión o comercialización. Por ello, puede afirmarse que en la actualidad, la información del sector público es un componente importante del mercado de contenidos.

4.5 La evolución de las regulaciones sobre la información del sector público: del secreto a la comercialización de la información.

El uso de las tecnologías de la información y la comunicación en la difusión de la información del sector público ha dado lugar a la adopción de nuevas normas reguladoras del acceso a la información o, al menos, a plantear la necesidad de adoptar nuevas normas al respecto. Ya se ha comentado que la información del sector público ha tenido funciones diferentes a lo largo de

la historia, lo que ha provocado que la legislación sobre el acceso a la información del sector público haya variado adaptándose tanto a las nuevas funciones como a los nuevos mecanismos de recolección, almacenamiento, difusión y comercialización. Siguiendo a CERRILLO MARTÍNEZ[568], a grandes rasgos, podríamos delimitar tres grandes etapas diferentes que van desde el reconocimiento formal del secreto como principio propio de la actuación de las administraciones públicas hasta la puesta a disposición del mercado de la información del sector público para su explotación comercial, pasando por el principio de transparencia administrativa y del derecho de acceso a la información del sector público, la creación de servicios de información administrativa, así como el uso de las tecnologías de la información.

4.5.1 Del secreto administrativo a la transparencia de la administración pública

Durante siglos, las administraciones públicas han venido considerando que la información que recaban o producían en el ejercicio de sus funciones, tenía únicamente un interés interno y que, por lo tanto, los ciudadanos no tenían la necesidad de acceder a dicha información. Desde la óptica de una organización burocrática, la administración pública no tenía la necesidad de informar a los ciudadanos de sus acciones, evitando así la presión y el control por parte de los ciudadanos.

La administración burocrática se caracterizaba por el secreto y el distanciamiento que, en general, existía entre la administración y los ciudadanos. El secreto administrativo cumplía una clara función de

[568] Cerrillo i Martínez, A. (2006). La información del sector público: del acceso a la reutilización. En Cerrillo Martínez, A. y Galán Galán, A. (Coord.), *La reutilización de la información del sector público*. Granada: Comares.

separación de la administración en relación con la sociedad, plenamente acorde con los postulados del estado liberal de derecho[569].

Con la llegada de la democracia en España, se rompe con el tradicional secreto administrativo y se reconoce el derecho de acceso a los archivos y registros administrativos en la propia Constitución de 1978[570] . Y de hecho, con la amplitud con la que se configura el derecho de acceso en el texto constitucional se puede incluso sostener el reconocimiento del principio de transparencia en la actuación administrativa[571]. El principio de transparencia que prevé la Constitución está plenamente relacionado con otros principios básicos del sistema democrático como los de eficacia, seguridad jurídica y legalidad.

A pesar de este reconocimiento constitucional del derecho de acceso a los archivos y registros administrativos, pocas variaciones se produjeron en la actuación de las administraciones públicas hasta la aprobación de la Ley 30/1992, de 26 de noviembre,[572], que recogía hasta cuatro manifestaciones diferentes del derecho a obtener información administrativa lo que, a su vez, implica el reconocimiento de una obligación particular de facilitar información administrativa ante una solicitud en este sentido por parte de un ciudadano

---

[569] Fernández Ramos, S (1997). *El derecho de acceso a los documentos administrativos*. Madrid: Marcial Pons, pág. 21.

[570] Constitución Española. BOE núm. 311, de 29 de diciembre de 1978**,** Artículo 105 La ley regulará: a) La audiencia de los ciudadanos, directamente o a través de las organizaciones y asociaciones reconocidas por la ley, en el procedimiento de elaboración de las disposiciones administrativas que les afecten. b) *El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.* c) El procedimiento a través del cual deben producirse los actos administrativos, garantizando, cuando proceda, la audiencia del interesado.

[571] Mestre Delgado, J.F. (1998). El derecho de acceso a archivos y registros administrativos [análisis del artículo 105.b) de la Constitución] (2ª edición ampliada). Madrid: Civitas, pág. 33

[572] Ya se ha comentado que hablamos de una Ley actualmente derogada por la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. (BOE núm. 236, de 2 de octubre de 2015)

y, por otro, el establecimiento de un deber genérico de organizar los servicios competentes para facilitar la información a los ciudadanos[573].

4.5.2 Del acceso a la información a la difusión de la información del sector público

Reconocido jurídicamente el derecho a acceder a la información del sector público y desarrollado un sistema para canalizar las demandas y peticiones de los ciudadanos y las empresas para acceder a dicha información, la siguiente etapa de la evolución se caracteriza por la aparición de las tecnologías de la información y el comienzo y su incorporación en el desarrollo de la actividad informativa que llevan a cabo las administraciones públicas. Las tecnologías de la información y el conocimiento permiten facilitar a los ciudadanos mucha más información que la que se venía facilitando y de forma mucho más accesible.

Así, la utilización de Internet ha incrementado la accesibilidad de la información de las administraciones públicas. Cualquier ciudadano, independientemente del lugar donde se encuentre, puede acceder a cualquier información en poder de las administraciones públicas con sólo acceder a la página web de la administración pública.

Esta fase se caracteriza principalmente por ser la administración pública la que ofrece o distribuye la información sin necesidad de que haya una petición o solicitud expresa por parte de los ciudadanos. Además, el abanico de informaciones que se ponen a disposición de los ciudadanos, también se ha ido ampliando.

---

[573] Véase un desarrollo detallado de estos aspectos en Cerrillo i Martínez, A. (2000). Régimen jurídico de la información administrativa. En Tornos Mas, J. y Galán Galán, A. *La comunicación pública. La información administrativa al ciudadano*. Madrid: Marcial Pons, págs. 230 y sigs.

4.6 La aparición de nuevos protagonistas: el usuario y la intermediación de base tecnológica

Otra de las características de la modernización tecnológica se refiere a la presencia de un nuevo sujeto que realiza funciones de intermediación entre el usuario de la tecnología y el tratamiento de los datos.

Así sucede con quien desarrolla las aplicaciones informáticas, especialmente si son de uso gratuito, ya que normalmente se basan en un modelo de negocio en el que el pago tiene lugar a través de la autorización para llevar a cabo un tratamiento de la información del usuario; o, incluso, la cesión a otro sujeto, que será quien proceda a realizar una explotación comercial de los datos obtenidos, bien aisladamente bien a partir de su conexión con los que hubieses proporcionado otros usuarios o, en su caso, a través del contraste con ciertos parámetros previamente prefijados. Así, este tratamiento puede permitir la generación de información relevante, ya respecto de los propios sujetos de los que recogieron los datos ya, de manera genérica, en relación con la obtención de conclusiones que permitan plantear decisiones de mercado o relativas a la eficacia de ciertos tratamientos o productos.

4.6.1 Se facilita la interconexión de los sistemas de información

Afirma VALERO TORRIJOS[574] que resulta indudable que la tecnología supone una mayor interconexión potencial de los sistemas de información, de manera que se favorece la accesibilidad a los datos y asimismo se permite que se puedan actualizar o, en su caso, contrastar con los que obran en poder de otros usuarios o entidades de procesamiento que se puede llevar a cabo de manera automatizada, es decir, sin intervención directa de personas físicas.

---

[574] Valero Torrijos, J. (2014). Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria. Implicaciones jurídicas desde la perspectiva de la innovación tecnológica. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Aranzadi.

La capacidad de almacenamiento de los equipos informáticos y la velocidad de transmisión de las actuales redes permites conexiones masivas y automatizadas, big data, que, además, se llevan a cabo por cauces no formalizados aprovechando la apertura de los datos sectoriales gracias a las numerosas políticas de open data que se están implementando en los últimos años al amparo del denominado Gobierno Abierto[575], así como debido a la ingente información de libre acceso disponible en Internet.

En consecuencia, los controles y limitaciones propios de las cesiones de datos personales resultan manifiestamente inadecuados[576], siendo preciso abordar un replanteamiento en cuanto a las garantías establecidas para la tutela de los distintos bienes jurídicos en juego, tan to públicos como privados.

En efecto, al incorporarse la información a soporte electrónico y simplificarse notablemente el acceso a través de medios telemáticos, se plantea un nuevo escenario, donde las posibilidades de su reutilización se amplían notablemente.

Cuando los datos se encuentran en soporte papel, su vinculación con otros para la obtención de información de valor añadido resulta ciertamente compleja, ya que dicha operación ha de llevarse a cabo supuesto por supuesto, y de forma manual, dificultándose la opción de implantar tratamientos automatizados a menos que tenga lugar dicho procesamiento previo. Sin embargo, el uso de estándares adecuados, nos sitúa ante un escenario en el que esa labor se simplifica notablemente y, en

---

[575] Por lo que se refiere a las implicaciones jurídicas de este fenómeno, véase Cotino Hueso, L. (2013). Derecho y "Gobierno Abierto", La regulación de la transparencia y la participación y su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones Públicas. Propuestas concretas. En Bermejo Latre, J.L. y Castel Gayan, S (eds.), *Transparencia, participación ciudadana y administración pública en el siglo XXI*. Zaragoza: IAAP, pp. 51 y ss.

[576] Véase Valero Torrijos, J. (2013). Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado. En Valero Torrijos, J. (Coord..). *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Navarra: Aranzadi, pp. 53 a 58.

consecuencia, se facilita el tratamiento automatizado de los datos, desplazándose el control en el acceso y posterior uso de la información de quien tiene inicialmente en su poder, a quien diseña y desarrolla la correspondiente aplicación informática. Y precisamente aquí radica uno de los ejes a partir del cual tratar de superar las dificultades que, desde el punto de vista de las limitaciones jurídicas, conlleva la normativa sobre el acceso y la reutilización de la información.

4.6.2 El potencial carácter masivo de los tratamientos de información

La actual sociedad tecnológica se caracteriza por la enorme cantidad de información que se maneja, lo que unido al potencial de las comunicaciones permite llevar a cabo tratamientos masivos de datos a partir de los que obtener información de enorme interés, tanto por lo que se refiere a su vinculación con sujetos concretos como, asimismo, desde una perspectiva general para analizar tendencias y comportamientos reiterados que permitan adoptar decisiones más generales en cuanto a su ámbito y sus objetivos.

Desde la perspectiva de esta modalidad de uso avanzado de la información, el big data nos sitúa ante un escenario complejo al que hemos de enfrentarnos teniendo en cuenta las singularidades de las actividades en relación con las cuales pretende realizarse el tratamiento de los datos, si bien a los efectos del régimen jurídico aplicable deberían tenerse en cuenta los destinatarios y el fin de los servicios sobre los que se pretenda proyectar el resultado del tratamiento informativo. Las tendencias más recientes[577] nos sitúan ante un modelo de gestión de la información basado en el aprovechamiento de la utilidad de los datos a la hora de ofrecer servicios de valor añadido.

[577] Batini, C. (2010). Data Governance. En G. Viscusi, C. Batini y M. Mecella, *Information Systems for eGovernment*, Heidelber: Springer–Verlag, p. 21.

1.1.1.1 Del acceso a la información en poder de las Administraciones Públicas al open data: caracterización general

Siguiendo a VALERO TORRIJOS, desde la perspectiva de la innovación tecnológica, el acceso y la difusión de la información administrativa se ha de enfocar necesariamente a partir de los planteamientos del denominado *open data*, cuyo impulso en los últimos años ha tenido lugar desde la normativa sobre reutilización de la información del sector público.

En el actual contexto económica y político, la demanda social de una Administración más transparente aboca a planteamientos de Gobierno Abierto, de manera que las diferentes obligaciones informativas no solo han de articularse a través de medios electrónicos, siguiendo el modelo de la LTBG sino que, de forma inexcusable, han de adaptarse a las características propias del modelo open data[578].

Ahora bien, la consolidación de este modelo no solo requiere que la información se encuentra accesible por medios electrónicos ya que, aun siendo una elemental exigencia, resulta manifiestamente insuficiente si se

---

[578] Este autor nos detalla las características principales de este modelo de difusión de la información en poder de las Administraciones Públicas. Así, se trata de un modelo en el que: «i) el destinatario final no acceder directamente a la información en poder de la Administración Pública que dispone de los datos, sino que, por el contrario, lo hace a través de un intermediario –el agente reutilizador– que le presta un servicio, en la medida que convierte la mera información y los datos brutos en conocimiento de utilidad; ii) el usuario final de la información ya no requiere formular una solicitud a la entidad pública utilizando los cauces forales de los registros administrativos, ni tampoco se ha de tramitar un procedimiento, siendo preciso acudir a otras herramientas que permitan gestionar de forma más dinámica las autorizaciones de acceso y reutilización, tal y como sucede con las licencias previas; y iii) la determinación de las circunstancias que impiden el acceso a la información han de fijarse previamente –tal y como sucede con las relativas a la protección de la intimidad y los datos personales de los pacientes– ya que, de lo contrario, el servicio no podría prestarse en las condiciones técnicas y jurídicas necesarias para satisfacer al usuario final. El acceso ha de producirse en unas determinadas condiciones técnicas ya que, en última instancia, no se trata simplemente de acceder a la información sino, más bien, de que el intermediario puede ofrecer servicios de valor añadido a partir de los datos obtenidos de la Administración». Valero Torrijos, J. (2014). Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria. Implicaciones jurídicas desde la perspectiva de la innovación tecnológica. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Aranzadi.

pretende llevar a cabo una gestión avanzada de la misma que permita incorporarle un valor añadido basado en la innovación de los servicios que se pretenden ofrecer. Así pues, no basta con que se reconozca el derecho de acceso a la información por medios telemáticos y, en consecuencia, que los datos se encuentran en soporte electrónico, sino que, además, han de estarlo en unas condiciones determinadas:

> *«i) que sean susceptibles de un tratamiento automatizado por parte del reutilizador; ii) que no se impongan restricciones injustificadas por lo que respecta a los fines de los usos posteriores; y, sobre todo, iii) que la reutilización tenga lugar de manera gratuita o, en su caso, atendiendo al coste marginal que conlleva la difusión»*[579].

Ciertamente, desde el punto de vista normativo, las obligaciones para las Administraciones Públicas en orden a ofrecer sus datos bajo tales condiciones son insuficientes, hasta el punto de que la letra c) del artículo 11 LTBG, al hablar de los principios técnicos, únicamente contempla que se fomente la publicación de la información en formatos que permitan su reutilización.

1.1.1.2 Las singularidades del big data

Dos notas distintivas especialmente destacadas pueden apuntarse inicialmente en relación con el big data: de una parte, la mayor exigencia de transparencia que requiere y/o supone a pesar de las limitaciones del marco normativo vigente y las reticencias que inspiran la práctica administrativa; y, de otra, la necesidad de proceder a una redefinición de las relaciones entre las Administraciones Públicas, los ciudadanos, y los prestadores de servicio.

Se ha mantenido en relación al *big data* que es la próxima frontera para la innovación, la competitividad y la productividad. Esta afirmación se basa en

---

[579] Valero Torrijos, J. (2014). Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria. Implicaciones jurídicas desde la perspectiva de la innovación tecnológica. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Aranzadi.

la evidencia de que los medios tecnológicos actualmente disponibles permiten llevar a cabo tratamientos de la información que exceden la capacidad de procesamiento de las herramientas de software de datos convencionales en relación con la captura, almacenamiento, gestión y análisis, de manera que la obtención de un valor añadido de los datos requiere la utilización de formas alternativas para su tratamiento[580]. Esta exigencia se basa en el incremento sustancial tanto del volumen de información que se maneja, la velocidad con que se hace y, asimismo, la variedad de los datos y las fuentes de información[581]. No se trata simplemente de una simple agregación cuantitativa de tales variables sino, sobre todo, cualitativa, ya que el incremento en el número de datos que se procesan conlleva igualmente una mayor exactitud en el tratamiento de la información; y del mismo modo, el aumento exponencial de las fuentes de donde se obtienen los datos permite identificar las que ofrecen información de interés, descartando los datos irrelevantes. Y todo ello de manera prácticamente instantánea en muchos casos, lo que facilita la adopción automatizada de decisiones.

Quizás el aspecto más destacado de la revolución que supone el big data consiste en la unificación de grandes conjuntos de datos con un análisis avanzado que permite resolver problemas y buscar alternativas basándose en el uso de potentes algoritmos y aprovechando las posibilidades de aprendizaje de las máquinas.

4.6.3 La segregación de los datos del documento donde se encuentran: una premisa inexcusable para su tratamiento avanzado

El uso avanzado de medios electrónico permite desvincular los datos del documento original donde se contengan y, de este modo, llevar a cabo su

---

[580] Dumbill, E. (2012). Getting up to Speed with Big Data. En *Big Data Now: 2012 Edition*. Sebastopol: O´Reilly Media, Inc, p. 3.

[581] Ibídem, pp. 4 a 8.

procesamiento independiente[582], si bien resulta esencial que las garantías generales de los documentos en cuanto a integridad y autenticidad pueden asegurarse incluso cuando se incorporen a otros documentos o sean objeto de tratamiento. Así pues, el documento como unidad de gestión ha de fragmentarse en atención a la información que contiene, de manera que solo se pongan a disposición de terceros aquellos datos que sean estrictamente necesarios para el ejercicio de sus funciones o la satisfacción de sus derechos o intereses legítimos. Incluso, puede darse el caso de que no sea necesario a tales efectos compartir la información original, sino que, por el contrario, baste con una versión transformada de la misma que no conlleve una modificación esencial, de manera que dicha exigencia legal se vería incluso reforzada en su garantía. Esta posibilidad sería de gran utilidad en aquellos supuestos en que, como sucede en el ámbito específico de la investigación biomédica, se requiera el consentimiento específico del titular de los datos para su cesión incluso una vez ya disociados.

Asimismo, la puesta a disposición segmentada a partir de la información relevante y no de los documentos, entendidos como conjuntos estructurados dotados de unidad que no se pueden fragmentar, permite limitar el acceso a la información a fin de lograr la protección efectiva de derechos e intereses públicos o privados que deban respetarse, tal y como sucede con la intimidad la seguridad pública o, incluso, los datos de carácter personal que, aun sin ser íntimos, no esté justificada su revelación.

Como conclusión VALERO TORRIJOS detalla que este tipo de planteamientos de gestión avanzada han de superar una difícil barrera: la realidad actual en las Administraciones Públicas parte en gran medida de un modelo de gestión documental diseñado fundamentalmente para el ámbito de cada entidad; limitación que ha de considerarse superada, en particular si tenemos en cuenta las mayores necesidades suscitadas a la hora de compartir información como consecuencia de las posibilidades que ofrece la

---

[582] En relación a las implicaciones jurídicas de este paradigma en el ámbito general de las Administraciones Públicas, véase Valero Torrijos, J. (2013). *Derecho, innovación y Administración electrónica*. Sevilla: Derecho Global, pp. 293 a 303.

tecnología y, asimismo, la complejidad organizativa propia de un modelo político-administrativo descentralizado. Así pues, la información ha de generarse o, en su caso, incorporarse a loa archivos administrativos en un determinado formato que permita su posterior tratamiento automatizado a partir del sometimiento a estándares de interoperabilidad generalizados, tal y como se está evidenciando en materia de reutilización comercial y *open data*[583].

583 Valero Torrijos, J. (2012). El acceso y la reutilización de la información administrativa. Implicaciones jurídicas del proceso de modernización tecnológica de las Administraciones Públicas en su actual y futura configuración», *Diario La Ley*, *7800*.

5 DIFERENCIAS ENTRE EL DERECHO DE ACCESO A LA INFORMACIÓN, LA PROTECCIÓN DE DATOS PERSONALES Y LA REUTILIZACIÓN DE LA INFORMACIÓN

Se ha afirmado en el primer capítulo de esta obra que el derecho de acceso a la documentación pública es reconocido ya en muchos ordenamientos y textos como un derecho fundamental de las personas, de igual modo que el derecho fundamental a la protección de los datos personales.

Por otro lado, y desde un punto de vista distinto, ya hemos visto que el derecho de acceso a los datos personales, que corresponde al sujeto titular de los datos, es el derecho a solicitar y a obtener gratuitamente información sobre sus datos de carácter personal sometidos a tratamiento, el origen y las comunicaciones de los mismos. Este derecho es una herramienta esencial para la garantía del derecho fundamental a la protección de datos, con el fin de poder controlar y decidir sobre el destinatario y los usos de la información que contiene datos relativos a una persona.

Ambos, son fundamento de las nuevas sociedades democráticas, el primero para garantizar la transparencia y la participación ciudadana, y el segundo, como requisito para el respeto a la autonomía individual, como herramienta para la garantía de la intimidad y para el pleno conocimiento de los datos disponibles sobre la persona individual por parte de cualquier agente, instrumento básico en una sociedad que dispone, cada día más, de infinidad de recursos tecnológicos para comunicar, almacenar y relacionar datos personales.

SOLERNOU VIÑOLAS[584] declara que un ejemplo de confusión existente en esta materia lo ofrecía el legislador español en la exposición de motivos de

[584] Solernou Viñolas, A. (2006). Los datos personales como límite a la reutilización de la información del sector público. En Cerrillo i Martínez, A. y Galán Galán, A. (Coord.): *La reutilización de la informació del sector público*. Granada: Comares. p 100.

la primera Ley Orgánica que regulaba la protección de los datos personales en el Ordenamiento Jurídico español[585]. Resulta evidente que el contenido de estos derechos y su propia definición no se diferencia fácilmente. Del actual contexto, parece deducirse que el artículo 105.b) de la Constitución se refiere al derecho de acceso a la información de las entidades que integran el sector público como herramienta de participación y para la transparencia del funcionamiento de las mismas, mientras que la vigente Ley Orgánica de protección de datos de carácter personal[586], integra el *habeas data* juntamente con el derecho de rectificación, de cancelación y de oposición, como facultad imprescindible de los titulares para el control de los flujos de la información que les concierne[587].

---

[585] El apartado tercero in fine de la Exposición de motivos de la Ley orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal, BOE núm. 262, de 31 de octubre de 1992, en la actualidad derogada por la vigente Ley orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, establecía: «en concreto, los derechos de acceso a los datos, de rectificación y de cancelación, se constituyen como piezas centrales del sistema cautelar o preventivo instaurado por la Ley. El primero de ellos ha cobrado en nuestro país, incluso, plasmación constitucional en lo que se refiere a los datos que obran en poder de las Administraciones Públicas (artículo 105.b). En consonancia con ello queda recogido en la Ley en términos rotundos, no previéndose más excepciones que las derivadas de la puesta en peligro de bienes jurídicos en lo relativo al acceso a los datos policiales y a los precisos para asegurar el cumplimiento de las obligaciones tributarias en lo referente a los datos de este carácter, excepciones ambas que pueden entenderse expresamente recogidas en el propio precepto constitucional antes citado, así como en el Convenio Europeo para la protección de los Derechos Fundamentales.» M. Fernández Salmerón (2003). *La protección de los datos personales en las Administraciones Públicas*. Thomson Civitas. Navarra, pág. 168.

[586] El derecho de acceso se define en el artículo 15.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. (BOE núm 298 14/12/1999) en los siguientes términos: «1. El interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos. 2. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos. 3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes».

[587] A este respecto, Fernández Salmerón afirma expresamente «por lo que se refiere a la primera de las confusiones, puede que a muchos resulte elemental señalar que los derechos de acceso que regulan por un lado la LRJPC y, por otro, la LOPD son distintos en su causa, funcionalidad y régimen, pero

En puridad, ambos son derechos a proteger sin existir ninguna relación de jerarquía entre ellos, y en la mayoría de los supuestos, no hay tensión entre ambos derechos[588]. No obstante, en determinados contextos, pueden ser invocados al mismo tiempo, supuestos en que será necesario el análisis de

---

no está de más desarrollar un ejercicio de pedagogía que, por otra parte, a alguien podrá siempre ayudar. La de acceso que regula el artículo 15 LOPD (Cuya disciplina viene desarrollada en la Instrucción 1/1998, de 19 de enero, de la Agencia de Protección de Datos, relativa al ejercicio de los derechos de acceso, rectificación y cancelación. BOE núm. 25, de 29 de enero de 1998) es una de las facultades que integran el derecho a la protección de datos personales y a través de él el titular de los datos puede desplegar un seguimiento sobre los relativos a su persona, consistiendo cabalmente tal derecho en la posibilidad de conocimiento de los datos que afectándole, obren en poder del sujeto interpelado –no necesariamente, por tanto, de una Administración Pública, lo que constituye una nota distintiva más en relación con el derecho de acceso administrativo–, excluyendo, pues, los datos personales relativos a un tercero. Por el contrario, el derecho de acceso a los documentos administrativos tiene por objeto obtener determinada información que puede o no ser personal, pero en el caso de que lo sea, de ordinario estará directamente vinculada a una tercera persona, raramente al solicitante. Adicionalmente podría cuestionarse –y esto es determinante– que, cuando el acceso a los documentos administrativos afecte a informaciones personales, ambos derechos tengan el mismo objeto, pues mientras aquél se ejerce en general sobre "documentos" integrados en expedientes administrativos, el acceso en materia de protección de datos personales busca únicamente el conocimiento de éstos, prescindiendo del contexto en el que los mismos se han generado. No obstante, y por razones de coherencia en la sistemática expositiva, analizamos esta cuestión más adelante. En todo caso, todavía podrían añadirse algunas diferencias adicionales, relacionadas con la tutela de ambos derechos y derivadas en gran parte de la diversa configuración que adquieren en nuestro ordenamiento. De este modo, mientras que en el derecho de acceso en materia de protección de datos se instaura una relación jurídica bilateral, esto es, entre el solicitante del acceso y el titular o responsable del fichero o tratamiento, en el acceso administrativo la relación entre el solicitante y –cuando sea el caso– el titular del derecho a mantener la reserva de su información personal (cualquiera que sea la forma de tutela que tal derecho adopte: intimidad o protección de datos) se encuentra mediada por la Administración Pública titular de los documentos cuyo conocimiento se pretende, instaurándose así un vínculo trilateral en el marco de un procedimiento administrativo típico. De ello se deriva alguna importante conclusión, como la que postula que tal vez no estuviera de más que, en su calidad de interesado, en el procedimiento de acceso administrativo se diera audiencia, aun a riesgo de recargar el expediente, al titular del hipotético derecho a la reserva y que él mismo pudiera impugnar, por tanto, la eventual resolución que recayera en el procedimiento. Como se comprenderá, esta circunstancia no puede concurrir en ningún caso en el ejercicio del derecho de acceso ex artículo 15 LOPD. Sea como fuere, la clarificación conceptual pretendida exige necesariamente dar un paso más». «La difusión de información administrativa en Internet y la protección de los datos personales» de M. Fernández Salmerón y J. Valero Torrijos. El texto completo se encuentra accesible en http://www.avpd.euskadi.eus/contenidos/evento/4_encuentro_apds/es_intro/adjuntos/PONENCIA_MANUEL_FERNANDEZ.pdf

[588] Informe del Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. *Background Paper Series, 1*.

los bienes en juego. Por otro lado, la reutilización de la información del sector público o su explotación se proclama como un interés a perseguir, no se fundamenta en una obligación formal[589]. Las tecnologías de la información y la comunicación tienen un papel esencial en esta relación. Son ellas las herramientas más poderosas para la difusión de la información, pues son los instrumentos para una realización eficaz de la transparencia y el conocimiento, y a la vez deben ser cuidadosamente utilizadas para poder garantizar los derechos en juego. Justamente, su uso sin las debidas precauciones, puede llevar a daños irreparables en términos de intimidad, protección de datos personales o privacidad en general.

La yuxtaposición del derecho a la protección de datos de carácter personal y del derecho de acceso a la documentación pública se resuelve conforme a las reglas habituales de interpretación aplicables a los supuestos de colisión de derechos fundamentales, de acuerdo con el juicio de proporcionalidad que corresponde a los tribunales constitucionales, la ponderación del daño, o el test o balance del interés público[590]. De conformidad con el test del interés público se ponderará cuál de los derechos fundamentales prevalece sobre el otro, dado el supuesto concreto que se plantee y atendiendo a criterios de equilibrio para velar por el respeto de ambos.

Se ha de considerar que, en la mayoría de las ocasiones, tanto la reutilización como el derecho de acceso, implicarán la revelación de información para nuevas finalidades, ya sea para el ejercicio de la participación democrática o para la comercialización de la información. Así, la petición de acceso, el suministro de información, deberá analizar en todo

---

[589] Considerando 9 de la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, de 17 de noviembre de 2003, relativa a la reutilización de la información del sector público DOUE L 345 de 31/12/2003 «La presente Directiva no contiene la obligación de autorizar la reutilización de documentos. La decisión de autorizar o no la reutilización corresponderá a los Estados miembros o al organismo del sector público que corresponda […]»

[590] Solernou Viñolas, A. (2006). Los datos personales como límite a la reutilización de la información del sector público. En Cerrillo i Martínez, A. y Galán Galán, A. (Coord.): *La reutilización de la informació del sector público*. Granada: Comares. p 105.

caso, a priori, qué finalidad de destino tendrá la información, aunque este es un requerimiento que no exige la Directiva 2003/98/CE.

La reutilización de la información será en muchos casos autorizada únicamente para unos fines concretos y específicos y una desviación de los mismos podrá llevar aparejada una sanción. Sin embargo, cabe preguntarse si existen los mecanismos pertinentes para evitar que la reutilización de la información del sector público sea en perjuicio de otros derechos, y si puede revocarse la situación en aquellos casos en que, por ejemplo, no se haya autorizado un uso comercial y en cambio, se hayan explotado comercialmente los datos.

5.1 La relación entre la reutilización de la información y la protección de los datos personales

Para interpretar qué límites impone la protección de los datos personales a la reutilización, debemos partir de una perspectiva más amplia, más general, que considere así mismo, otros fundamentos que legitiman el acceso a la información del sector público, acceso en términos generales.

Debemos tener presente otro derecho de los particulares, nos referimos al derecho de acceso a los documentos de la administración en el marco de la libertad de información[591]. De esta forma, son tres los bienes o intereses que deben ser considerados ante cualquier petición o decisión que afecte el suministro de información elaborada o en manos de las entidades públicas: i) el derecho de acceso a la información del sector público en el marco de la libertas de información; ii) la protección de datos de carácter personal, que confiere al titular de los datos el derecho a acceder a la información que le

[591] La Directiva 2003/98/CE recoge expresamente en el Considerando 9, y en el apartado 3 de su artículo 1, que está basada en los actuales regímenes de acceso de los Estados miembros y no modifica las normas nacionales de acceso a documentos, ni las afecta de forma alguna.

concierne[592]; y iii) la reutilización de la información del sector público con arreglo a la Directiva 2003/98/CE.

Por otro lado, la Directiva 95/46/CE autoriza[593] que se tenga en cuenta el principio de acceso público a los documentos oficiales a la hora de aplicar los principios expuestos en ella. La relación entre estas tres materias o regímenes distintos es evidente y expresa en las remisiones que entre ellos existen.

No obstante, el análisis de la relación entre protección de los datos personales y la reutilización, no nos ofrece una respuesta genérica y unívoca. No hay una habilitación general posible, ni una relación detallada y exhaustiva de supuestos autorizados y de supuestos prohibidos. Deberá realizarse una valoración caso por caso, equilibrando los diferentes intereses yuxtapuestos, un juicio de proporcionalidad que permita integrar y complementar el respeto de los diferentes valores para garantizar su debido cumplimiento. En algunos casos, como resultado de esta valoración, el acceso a la información, para su reutilización o para el conocimiento general

---

[592] En el artículo 12 de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (DOCE L281 de 23.11.1995) se define el derecho de acceso del interesado a los datos, en los siguientes términos: «Los Estados miembros garantizarán a todos los interesados el derecho de obtener del responsable del tratamiento: a) libremente, sin restricciones y con una periodicidad razonable y sin retrasos ni gastos excesivos: - la confirmación de la existencia o inexistencia del tratamiento de datos que le conciernen, así como información por lo menos de los fines de dichos tratamientos, las categorías de datos a que se refieran y los destinatarios o las categorías de destinatarios a quienes se comuniquen dichos datos; - la comunicación, en forma inteligible, de los datos objeto de los tratamientos, así como toda la información disponible sobre el origen de los datos; - el conocimiento de la lógica utilizada en los tratamientos automatizados de los datos referidos al interesado, al menos en los casos de las decisiones automatizadas a que se refiere el apartado 1 del artículo 15; b) en su caso, la rectificación, la supresión o el bloqueo de los datos cuyo tratamiento no se ajuste a las disposiciones de la presente Directiva, en particular a causa del carácter incompleto o inexacto de los datos; c) la notificación a los terceros a quienes se hayan comunicado los datos de toda rectificación, supresión o bloqueo efectuado de conformidad con la letra b), si no resulta imposible o supone un esfuerzo desproporcionado. Por su parte, ya se ha hecho referencia al artículo 15.1 LOPD conforme al cual el interesado tendrá derecho a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos, así como las comunicaciones realizadas o que se prevén hacer de los mismos.

[593] Véase el Considerando 72 de la Directiva 95/46/CE.

de terceros, deberá ser restringido, ya sea en el mismo contenido de la información, con la disociación de los datos o la omisión de determinados contenidos, o con la propia restricción al acceso limitándolo a un determinado colectivo, para un determinado uso o previa la acreditación de un interés particular.

En principio, la relación entre el régimen de protección de datos personales y la regulación de la reutilización de la información del sector público es de no injerencia, de neutralidad[594]. Las obligaciones inherentes al régimen de protección de los datos de carácter personal subsisten en los supuestos en los que la documentación a reutilizar contenga datos personales.

La reutilización de la información del sector público, sea con finalidades comerciales o no, supone, en términos de la Directiva 95/46/CE y de las correspondientes normas nacionales de transposición, un cambio en la finalidad original. Otorgar un segundo uso o un uso adicional a unos datos personales que habían sido recabados, utilizados y conservados en ejercicio de funciones públicas, implica, per se, un nuevo tratamiento de datos de carácter personal.

---

[594] Así lo declara expresamente el apartado 4 del artículo 1 de la Directiva 2003/98/CE «La presente Directiva no menoscaba ni afecta en modo alguno el nivel de protección de las personas físicas en lo que respecta al tratamiento de datos personales con arreglo a las disposiciones del Derecho comunitario y nacional, y, en particular, no altera las obligaciones ni los derechos establecidos en la Directiva 95/46/CE.» En el mismo sentido, el Considerando 21 de la misma afirma «La presente Directiva se debe incorporar al Derecho interno y aplicar de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos» Por su parte, el Considerando 154 del RGPD establece que «la Directiva 2003/98/CE del Parlamento Europeo y del Consejo no altera ni afecta en modo alguno al nivel de protección de las personas físicas con respecto al tratamiento de datos personales con arreglo a las disposiciones del Derecho de la Unión y los Estados miembros y, en particular, no altera las obligaciones ni los derechos establecidos en el presente Reglamento. En concreto, dicha Directiva no debe aplicarse a los documentos a los que no pueda accederse o cuyo acceso esté limitado en virtud de regímenes de acceso por motivos de protección de datos personales, ni a partes de documentos accesibles en virtud de dichos regímenes que contengan datos personales cuya reutilización haya quedado establecida por ley como incompatible con el Derecho relativo a la protección de las personas físicas con respecto al tratamiento de los datos personales».

El Grupo del Trabajo del artículo 29 sobre protección de datos ha señalado[595] que la difusión a terceras partes de los datos personales que la administración ostenta tiene que ser considerando tratamiento de datos personales y que las previsiones de la normativa de protección de datos personales deberán ser consecuentemente respetadas, con independencia de cuál sea el modo particular que se utilice para su difusión, o del carácter público de los datos.

La definición de lo que entendemos por tratamiento de datos de carácter personal se establece en la Directiva 95/46/CE[596]. Así, este nuevo tratamiento de los datos, su reutilización, deberá ser analizado a la luz de los principios fundamentales del régimen de protección de los datos personales, el principio de legitimidad del tratamiento y el principio de calidad de los datos. Consecuentemente, el tratamiento deberá ser legítimo al amparo de lo que disponen los preceptos de aquella Directiva, al igual que lo fue el tratamiento original.

---

[595] El Dictamen 5/2001, sobre el Informe Especial del Defensor del Pueblo Europeo al Parlamento Europeo a raíz del proyecto de Recomendación dirigido a la Comisión Europea en la reclamación 713/98/IJH, de 17 de mayo de 2001, declara expresamente «los datos personales contenidos en un documento oficial o en poder de una administración u organismo público conservan este carácter personal, por lo que deben protegerse de acuerdo con la legislación en materia de protección de datos, en la medida en que el tratamiento de dichos datos pertenezca al ámbito de aplicación de esta legislación». Accesible en el siguiente link http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2001/wp44_es.pdf

[596] El concepto de tratamiento es definido por el apartado b) del artículo 2 de la Directiva 95/46/CE como «cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, y aplicadas a datos personales, como la recogida, registro, organización, conservación, elaboración o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma que facilite el acceso a los mismos, cotejo o interconexión, así como su bloqueo, supresión o destrucción». Por su parte, en el ordenamiento español, la definición de tratamiento de datos se encuentra en el apartado c) del artículo 3 de la LOPD, en los siguientes términos: «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.»

Con arreglo a la legislación española, la nueva utilización de los datos se regirá por los artículos 11[597] o 21[598] de la LOPD. Este mismo texto normativo define la cesión de datos de carácter personal como toda revelación de datos realizada a una persona distinta del interesado[599].

---

[597] Artículo 11. Comunicación de datos. «1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado. 2. El consentimiento exigido en el apartado anterior no será preciso: a) Cuando la cesión está autorizada en una ley. b) Cuando se trate de datos recogidos de fuentes accesibles al público. c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique. d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas. e) Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica. 3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar. 4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable. 5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley. 6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores».

[598] Artículo 21. Comunicación de datos entre Administraciones públicas. «1. Los datos de carácter personal recogidos o elaborados por las Administraciones públicas para el desempeño de sus atribuciones no serán comunicados a otras Administraciones públicas para el ejercicio de competencias diferentes o de competencias que versen sobre materias distintas, salvo cuando la comunicación hubiere sido prevista por las disposiciones de creación del fichero o por disposición de superior rango que regule su uso, o cuando la comunicación tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. 2. Podrán, en todo caso, ser objeto de comunicación los datos de carácter personal que una Administración pública obtenga o elabore con destino a otra. 3. No obstante lo establecido en el artículo 11.2.b), la comunicación de datos recogidos de fuentes accesibles al público no podrá efectuarse a ficheros de titularidad privada, sino con el consentimiento del interesado o cuando una ley prevea otra cosa. 4. En los supuestos previstos en los apartados 1 y 2 del presente artículo no será necesario el consentimiento del afectado a que se refiere el artículo 11 de la presente Ley.

[599] Véase el apartado i) del artículo 3 LOPD.

La intersección entre el régimen de protección de los datos personales y la reutilización o explotación comercial de la información del sector público, concurre únicamente en aquellos casos en que la información contiene datos personales. Serán muchos los supuestos en que la información pública a reutilizar no contenga más que información, en absoluto relacionada con las personas físicas. Sin embargo, el concepto de dato de carácter personal[600], es suficientemente amplio para que sea aplicable a un gran número de documentos en poder de los organismos del sector público.

El análisis de los límites que impone en derecho fundamental a la protección de los datos personales para la reutilización de la información del sector público, exige establecer una serie de directrices para interpretar aquellos supuestos en que la petición o la voluntad de reutilizar información de las administraciones públicas conlleven la difusión de datos de carácter personal. Nos encontramos ante supuestos en que será necesaria la ponderación de un interés general y un derecho fundamental: en primer lugar, la divulgación de la información para darle una nueva utilidad a unos documentos ya elaborados o producidos en el ejercicio de funciones públicas por parte de las entidades públicas, y en segundo lugar, la protección de la intimidad y el control de la información de las personas físicas que se ven reflejadas en los documentos, objeto de tutela del régimen de protección de los datos de carácter personal.

En términos generales, no se puede establecer una específica y puntual mención de los supuestos específicos que permitan la reutilización, en

---

[600] A la hora de definir los datos personales, el apartado 5) del Artículo 2 de la Directiva 2003/98/CE se remite a la definición contenida en la Directiva 95/46/CE. En ésta, por un lado, la definición la encontramos en el apartado a) de su artículo 2 en los siguientes términos: «toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social»; por otro, destacamos el Considerando 26, al establecer que «los principios de la protección deberán aplicarse a cualquier información relativa a una persona identificada o identificable; que, para determinar si una persona es identificable, hay que considerar el conjunto de los medios que puedan ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona […]».

concreto, si se da cumplimiento a las previsiones recogidas en los artículos 6[601] y 7[602] de la Directiva 95/46/CE, con las peculiaridades del régimen de protección de los datos sensibles establecidos en el artículo 8[603] de la misma, que en esencia requieren verificar el cumplimiento de los dos principios esenciales del régimen de protección de los datos, esto es, el principio de legitimidad del tratamiento y el principio de calidad de los datos, específicamente, el de limitación de los fines[604].

---

[601] El artículo 6 de la Directiva 95/46/CE expresamente tipifica que «1. Los Estados miembros dispondrán que los datos personales sean: a) tratados de manera leal y lícita; b) recogidos con fines determinados, explícitos y legítimos, y no sean tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando los Estados miembros establezcan las garantías oportunas; c) adecuados, pertinentes y no excesivos con relación a los fines para los que se recaben y para los que se traten posteriormente; d) exactos y, cuando sea necesario, actualizados; deberán tomarse todas las medidas razonables para que los datos inexactos o incompletos, con respecto a los fines para los que fueron recogidos o para los que fueron tratados posteriormente, sean suprimidos o rectificados; e) conservados en una forma que permita la identificación de los interesados durante un período no superior al necesario para los fines para los que fueron recogidos o para los que se traten ulteriormente. Los Estados miembros establecerán las garantías apropiadas para los datos personales archivados por un período más largo del mencionado, con fines históricos, estadísticos o científicos. 2. Corresponderá a los responsables del tratamiento garantizar el cumplimiento de lo dispuesto en el apartado 1».

[602] Al respecto, el artículo 7 de la Directiva 95/46/CE afirma que «los Estados miembros dispondrán que el tratamiento de datos personales sólo pueda efectuarse si: a) el interesado ha dado su consentimiento de forma inequívoca, o b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d) es necesario para proteger el interés vital del interesado, o e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva».

[603] Conforme el artículo 8 de la Directiva 95/46/CE, «los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad».

[604] Solernou Viñolas, A. (2006). Los datos personales como límite a la reutilización de la información del sector público. En Cerrillo i Martínez, A. y Galán Galán, A. (Coord.): *La reutilización de la informació del sector público*. Granada: Comares, p 108.

5.1.1 Límites a la reutilización: el principio de legitimidad del tratamiento

En primer lugar, es necesario garantizar la legitimidad de la difusión de los datos, la legitimidad del nuevo uso que implique la reutilización de la información. Como hemos visto anteriormente, es el artículo 7 de la Directiva 95/46/CE el que tipifica una lista cerrada de supuestos que permiten considerar legítimo cualquier tratamiento de datos personales.

Siguiendo sus postulados, podremos afirmar que la reutilización será legítima cuando el interesado la haya consentido[605] inequívocamente. La reutilización también estará legitimada cuando sea necesaria para la ejecución de un contrato, en el cual el interesado es parte o para la aplicación de medidas precontractuales adoptadas a petición del mismo. Difícilmente un contrato o convenio firmado por entidades públicas podrá obligar a la reutilización de datos personales sin que los afectados sean parte del mismo y que por tanto, hayan manifestado su voluntad en relación con el nuevo destino.

De igual modo, la letra c) del mismo artículo recoge que los datos personales pueden ser difundidos cuando el tratamiento resulte necesario para el cumplimiento de una obligación jurídica. Este argumento solo será aplicable cuando el organismo del sector público esté investido del poder específico para difundir los datos. Si la administración u organismo del sector público no tiene reconocida expresamente la competencia para difundir, comunicar o dar a conocer a terceros su información, este supuesto no será aplicable. No podemos perder de vista que no es posible invocar la Directiva 2003/98/CE como obligación jurídica que se tiene que cumplir, ya que ésta no genera ninguna obligación de difusión de la información personal[606]. La decisión corresponderá en cada caso a la autoridad competente que corresponda con arreglo al derecho interno.

---

[605] A efectos prácticos, se debería permitir al interesado prestar o denegar su consentimiento para la reutilización de los datos recabados, desde el mismo momento de la recogida.

[606] Tal y como reconoce el Considerando 9, ya visto con anterioridad.

El Grupo de Trabajo del artículo 29 sobre protección de datos considera[607] que, en relación con el supuesto previsto en el apartado e) del artículo 7 de la Directiva 95/46/CE que prevé la legitimidad del tratamiento cuando sea «necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos», hay una superposición con el supuesto que recoge el apartado c) del mismo artículo, al recoger la legitimidad cuando sea «necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento». La principal diferencia entre ambos apartados reside en el hecho de que en el supuesto en que el tratamiento sea necesario para el cumplimiento de una obligación jurídica, la legitimidad del tratamiento es apreciada por el legislador, mientras que en el caso en que el tratamiento sea necesario para cumplir una misión de interés público, la concurrencia y la legitimidad del caso corre a cargo del propio organismo público o autoridad pública, dejando, por lo tanto, un mayor margen de apreciación.

Finalmente, la Directiva prevé el supuesto f) del artículo 7, que establece una cláusula general que permite el tratamiento cuando éste «es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva». Esta cláusula exige que se realice, caso por caso, un test de equilibrio entre el derecho a la intimidad y el interés legítimo que persigue la reutilización. Se trata de una cláusula abierta a la posibilidad de permitir el tratamiento cuando el destino de los

[607] Dictamen 06/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE. WP217, de 9 de abril de 2014. El texto completo puede consultarse en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_es.pdf

datos sea legítimo y el *balance of interest*[608] aplicado al caso concreto, permita o justifique la reutilización de los datos, no inicialmente prevista.

En similares términos, el propio RGPD señala en su Considerando 154 que «el presente Reglamento permite que, al aplicarlo, se tenga en cuenta el principio de acceso del público a los documentos oficiales. El acceso del público a documentos oficiales puede considerarse de interés público. Los datos personales de documentos que se encuentren en poder de una autoridad pública o un organismo público deben poder ser comunicados públicamente por dicha autoridad u organismo si así lo establece el Derecho de la Unión o los Estados miembros aplicable a dicha autoridad u organismo. Ambos Derechos deben conciliar el acceso del público a documentos oficiales y la reutilización de la información del sector público con el derecho a la protección de los datos personales y, por tanto, pueden establecer la necesaria conciliación con el derecho a la protección de los datos personales de conformidad con el presente Reglamento».

Una vez evaluada la legitimidad de la reutilización, debe analizarse el cumplimiento del segundo principio, eje principal de todo el régimen de

---

608 El concepto «balance of interest» deriva del apartado f) del artículo 7 de la Directiva 95/46/CE interpretado con el Considerando 30 de la misma en los siguientes términos «para ser lícito el tratamiento de datos personales debe basarse además en el consentimiento del interesado o ser necesario con vistas a la celebración o ejecución de un contrato que obligue al interesado, o para la observancia de una obligación legal o para el cumplimiento de una misión de interés público o para el ejercicio de la autoridad pública o incluso para la realización de un interés legítimo de una persona, siempre que no prevalezcan los intereses o los derechos y libertades del interesado; que, en particular, para asegurar el equilibrio de los intereses en juego, garantizando a la vez una competencia efectiva, los Estados miembros pueden precisar las condiciones en las que se podrán utilizar y comunicar a terceros datos de carácter personal, en el desempeño de actividades legítimas de gestión ordinaria de empresas y otras entidades; que los Estados miembros pueden asimismo establecer previamente las condiciones en que pueden efectuarse comunicaciones de datos personales a terceros con fines de prospección comercial o de prospección realizada por una institución benéfica u otras asociaciones o fundaciones, por ejemplo de carácter político, dentro del respeto de las disposiciones que permiten a los interesados oponerse, sin alegar los motivos y sin gastos, al tratamiento de los datos que les conciernan», y permite legitimar el tratamiento de datos personales cuando es necesario para la realización de un interés legítimo de una persona, siempre y cuando no prevalezcan los intereses o los derechos y libertades del interesado.

protección de los datos personales: el principio de calidad de los datos personales. Ambos principios son acumulativos, se han de cumplir los dos.

5.1.2 Límites a la reutilización: el principio de calidad

Conforme a las estipulaciones del artículo 6 de la Directiva 95/46/CE, el principio de calidad exige que el tratamiento sea leal y lícito, y que los datos sean adecuados, pertinentes y no excesivos para el fin específico al que se tenga que destinar la reutilización. Este principio impide reutilizar datos cuando la finalidad pueda ser atendida con información anónima.

Este principio lleva aparejado el principio de limitación de los fines, que exige que los datos sean recogidos para fines determinado e impide que sean tratados con posterioridad de forma incompatible con éstos.

Para evaluar la compatibilidad se debe atender, en primer lugar, a las expectativas razonables de los afectados a fin de saber si, teniendo en cuenta el motivo por el cual fueron recabados los datos personales del interesado, cabe, dentro de unas expectativas razonables[609], su reutilización para atender un nuevo uso. Para el análisis de compatibilidad es necesario, así mismo, ponderar los intereses en juego. Nos referimos a valorar si el interés de la reutilización es suficientemente relevante para sacrificar el nivel de protección de los datos personales, o si por el contrario, no impone ningún límite al derecho de los afectados. Para determinar la compatibilidad es exigible un estricto análisis tanto de la finalidad original para la cual los datos fueron recogidos, como de la finalidad de destino, el fin que persigue la reutilización. Por tanto, realizar una definición lo más precisa posible de la finalidad original del tratamiento, es fundamental para poder determinar en una fase inicial, cuáles son sus usos legítimos, y qué difusión cabe hacer de los mismos.

---

[609] Las Administraciones Públicas recaban y conservan grandes cantidades de datos personales que son de suministro obligado por parte de los particulares. Por tanto, en las expectativas de las personas que se han visto obligadas a suministrar datos a las mismas, la reutilización debe cumplir con criterios de razonabilidad muy estrictos.

Debemos reparar en que todas las administraciones y entidades públicas, se encuentran sometidas, en el ejercicio de sus actuaciones, al principio de legalidad. Consecuencia de éste, todos los datos personales que las administraciones recaben y traten, deben obedecer al ejercicio de sus funciones públicas, legalmente atribuidas. De otro modo, las administraciones públicas ostentarían datos personales sin disponer de la habilitación necesaria para su tratamiento. Una definición vaga e imprecisa de las finalidades originales del tratamiento de los datos, conlleva dudas sobre su legalidad, y al mismo tiempo, dificultades para determinar las posibilidades de reutilización que tiene esta información.

En relación con la finalidad de destino, he de afirmar que no nos hallamos ante una exigencia recogida en la Directiva 2003/98/CE el conocer a priori cuál es el fin de la reutilización. Aquella no establece ninguna obligación jurídica, y únicamente señala que será el órgano competente el que deba resolver sobre la reutilización de cada documento. En cambio, el fundamento básico de la protección de los datos personales exige el conocimiento de los fines para los que los datos son objeto de tratamiento. Por consiguiente, siempre que la reutilización comprenda documentos que contengan datos personales, el fin de destino deberá ser conocido y expresamente autorizado.

En algunos sectores específicos, la finalidad de destino puede estar investida de legitimidad en atención a terceros derechos constitucionales. Nos estamos refiriendo al supuesto de la comunicación de la información a periodistas o a parlamentarios que requieran el acceso en ejercicio de las funciones constitucionalmente atribuidas, y en pleno respeto a derecho fundamentales como la libertad de prensa o de opinión.

Mención empresa merece también la declaración por parte del propio legislador de la compatibilidad, siempre y cuando se cumpla con las debidas garantías, de los tratamientos con fines históricos, científicos o estadísticos. Asimismo, debe tenerse en cuenta que la reutilización de la información que proviene de registros públicos o que ya se ha hecho pública por parte de la administración, también encontrará sus límites en los fines y en la calidad

de los datos personales que incluya[610]. En la mayoría de los registros públicos, la difusión de la información que contienen suele estar destinada a fines muy limitados, ya que la propia existencia del registro público, obedece a la atención de una finalidad específica; si los datos que contiene deben ser reutilizados para un determinado uso, la norma que define las finalidades y usos de la información registral, deberá precisar claramente qué formas de reutilización se admiten de la misma.

Por último, destacar que la evaluación del cumplimiento del principio de calidad, no corresponde solo a la autoridad del sector público que comunica o defiende los datos personales, sino también al tercer destinatario, que a efectos de la Directiva 95/46/CE, actuará como responsable del tratamiento y como tal, tendrá que cumplir con las correspondientes obligaciones. De esta manera, el análisis concreto sobre so la reutilización de un documento es respetuosa con el régimen de protección de los datos, corresponde no únicamente a la administración o entidad que ostenta la documentación, sino a cualquier destinatario que quiera dar un nuevo uso o un valor añadido a la información elaborada o recabada *ab initio* en ejercicio de funciones públicas, sea una empresa privada, un particular u otras entidades del sector público, cuando quedan incluidas en el ámbito de aplicación de la Directiva 2003/98/CE.

---

[610] Así, el Grupo de Trabajo del artículo 29, en el Dictamen 3/1999 relativo a Información del sector público y protección de datos personales. Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado "La información del sector público: un recurso clave para Europa" COM(1998) 585, de 03 de mayo de 1999, declara expresamente que «el legislador, cuando desea que un dato se vuelva accesible al público no considera sin embargo que haya de convertirse en res nullius. Tal es la filosofía del conjunto de nuestras legislaciones. El carácter público de un dato de carácter personal, resulte de una normativa o de la voluntad de la propia persona a la que alude el dato, no priva, ipso facto y para siempre, a dicha persona de la protección que le garantiza la ley en virtud de los principios fundamentales de defensa de la identidad humana». Accesible en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1999/wp20_es.pdf

5.1.3 Particularidades por razón de la naturaleza de los datos o del país de destino y por la finalidad del tratamiento.

Existen determinadas particularidades en relación a los datos sensibles, aquellos que revelan el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. Cuando la reutilización afecte a los denominados datos sensibles, la regla general es una prohibición de tratamiento. Será necesario solicitar el consentimiento explícito de los afectados en estos supuestos, pues difícilmente la reutilización de documentos que contienen datos sensibles o especialmente protegidos, podrá subsumirse en alguna de las excepciones al consentimiento previstas por los apartados siguientes del artículo 8 de la Directiva 95/46/CE. En el ordenamiento jurídico español, es el artículo 7 LOPD el que establece el excepcional régimen de protección de los datos sensibles, con las particularidades para los datos relativos a la salud que prevé su artículo 8.

De igual modo, deben tenerse en cuenta las reglas de autorización y habilitación de las transferencias internacionales cuando la reutilización recaiga en alguno de los supuestos en que es aplicable el régimen de las transferencias internacionales, sin que con ello se incluya todo supuesto en que la información quiera ser divulgada por Internet[611], pero sí aquellos supuestos en que la autorización o la comercialización implique la cesión de los datos a países de fuera del Espacio Económico Europeo.

Por último, cuando la reutilización de los datos personales en manos de las administraciones públicas tenga como destino su explotación comercial, el equilibrio entre el derecho fundamental a la protección de los datos personales de los afectados y los intereses comerciales de los operadores privados, tiende a decantarse claramente a favor de la protección de los particulares. Es difícil concebir la explotación comercial de bases de datos

---

[611] Véase al respecto la Sentencia Tribunal de Justicia de las Comunidades Europeas, Caso Lindqvist. Sentencia de 6 de noviembre de 2003.

personales de los particulares, que fueron recogidos para la ejecución de funciones públicas, sin que medie el consentimiento del afectado.

CAPÍTULO Vº: TRANSPARENCIA Y PROTECCIÓN DE DATOS

SUMARIO: 1 LÍMITES A LA TRANSPARENCIA Y AL ACCESO A LA INFORMACIÓN.–1.1 Introducción.–1.2 El derecho a la protección de datos como límite a la transparencia.–1.3 El potencial conflicto: dos derechos de rango constitucional y desarrollo legal con un punto de conexión, la divulgación por las autoridades públicas de información que contiene datos personales.–1.4 Aproximación al tratamiento de la transparencia en la Unión Europea. Su evolución desde la incipiente idea de política pública asociada a la realización del mercado.–1.4.1 La transparencia en la reutilización de la información del sector público. Especial referencia a la evolución que supone la Directiva 2013/37/UE.–1.4.2 Acceso del público a los documentos y protección de datos en el Derecho comunitario. Especial referencia al Reglamento (CE) núm 1049/2001, del Parlamento y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión y al Reglamento (CE) núm 45/2001, del Parlamento y del Consejo, de 18 de diciembre de 2001, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.–2 EL ÁMBITO DE APLICACIÓN DE LA LEY DE TRANSPARENCIA Y SU RELACIÓN CON LA LOPD.–2.1 Principio de publicidad, tratamiento y cesiones de datos personales.–2.2 Responsables de ficheros y sujetos obligados. Accountability y Transparencia.–2.3 Acceso a los datos personales e interés legítimo en el tratamiento.–3 TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES. CRITERIOS LEGALES DE CONCILIACIÓN.–3.1 El contenido del derecho a la protección de los datos de carácter personal.–3.2 La delimitación de los conflictos entre transparencia y protección de datos.–3.3 La articulación de las relaciones entre transparencia y protección de datos en la Ley 19/2013, de 9 de diciembre.–3.4 Los parámetros de resolución de conflictos previstos en el artículo 15 de la Ley de Transparencia.–3.5 La colaboración entre la Agencia Española de Protección de Datos y el Consejo de la Transparencia y Buen Gobierno.

1 LÍMITES A LA TRANSPARENCIA Y AL ACCESO A LA INFORMACIÓN

1.1 Introducción

La transparencia de los poderes públicos y la protección de los datos personales son dos pilares esenciales para la configuración de las actuales sociales de la información como verdaderas sociedades democráticas en las que, al mismo tiempo que se fomenta el control eficaz de la actuación de los gobernantes y la participación de la ciudadanía en los asuntos públicos, se protegen y se respetan de manera adecuada los derechos y libertades de los individuos, en particular los relacionados con la esfera personal y el libre

desarrollo de la personalidad. De este modo, afirma RODRÍGUEZ ÁLVAREZ, nos encontramos ante una exigencia que deriva directamente del principio democrático, que demanda una completa rendición de cuentas de los gobernantes ante la ciudadanía en relación con todas sus actuaciones con relevancia pública[612].

En palabras del profesor GUICHOT REINA, el presupuesto de la expansión de las leyes de acceso ha sido la consideración de que solo mediante la información pueden los ciudadanos participar en la vida pública con conocimiento cabal, influir en su desarrollo y prevenir y controlar las ineficiencias, los errores o las arbitrariedades que la actividad pública puede generar. La información contenida en los documentos administrativos y, en general, toda la información en manos de los organismos públicos, constituye una fuente de conocimiento de primera magnitud para la participación eficaz de los ciudadanos en los procesos democráticos. La consecuencia que se obtiene de todo ello es la mejora de la propia gestión pública y una profundización en la democracia y, en general, en el funcionamiento social y económico de los Estados, en un círculo virtuoso[613]. En consecuencia, el principio de transparencia y el derecho de acceso a la información favorecen la participación en los asuntos públicos, fortalecen el control democrático del poder y contribuyen a lograr una mayor objetividad e imparcialidad en el funcionamiento de los entes públicos. De ahí que el parámetro que en cada Estado determine el nivel de acceso a la información pública sea un indicador muy relevante del grado de democracia efectiva, de la cuota de democracia real de la respectiva sociedad.

A su vez, el derecho a la intimidad surge como protección de un reducto último de reserva del individuo frente al conocimiento ajeno, el "derecho a

---

612 Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, p. 53.

613 Guichot Reina. E. (2012). Transparencia versus Protección de Datos. En Blasco Esteve A. (Coord) El Derecho Público de la crisis económica. Transparencia y Sector Público. Hacia un nuevo Derecho Adminsitrativo. Madrid: INAP, p. 285.

ser dejado en paz"[614]. Con posterioridad, el surgimiento de la informática, con su potencial inagotable de almacenamiento y cruce de datos, da origen a las normas sobre protección de datos personales, que pretenden garantizar el control de las personas sobre su propia información, el derecho a la llamada "autodeterminación informativa"[615]. Así, el derecho fundamental a la protección de los datos personales está adquiriendo cada vez más relevancia práctica en las sociedades actuales, caracterizadas por estar cada vez más tecnologizadas e interconectadas, en las que día a día se incrementa el volumen de información personal que se genera y, al mismo tiempo, se van perfeccionando las capacidades técnicas para recopilar, almacenar, analizar y utilizar esa información con fines muy diversos. Este uso cada vez más intenso de los datos personales trae consigo un constante incremento de los riesgos que afectan a la esfera personal de los individuos. En este contexto de nuevas y crecientes amenazas es primordial fortalecer las garantías que el derecho a la protección de datos, en cuanto poder de autodeterminación sobre la información personal, concede a todas las personas para asegurar la salvaguarda de los derechos fundamentales más relacionados con el libre desarrollo de la personalidad.

---

[614] Dembitz Brandeis, L. y Warren S. D. (1890). The right to privacy. *Harvard Law Review, vol. IV, 5.*. De hecho, no es casual que el primero de estos autores, Louis D. Brandeis, refleje en su libro *Dembitz Brandeis, L. (1914). Other People´s Money and How the Bankers Use It,* p. 92, la celebérrima frase «Publicity is justly commended as a remedy for social and industrial diseases. Sunlight is said to be the best of disinfectants; electric light the most efficient policeman», traducida como "La publicidad es justamente elogiada como un remedio para las enfermedades sociales e industriales. La luz del sol se dice que es el mejor de los desinfectantes; la luz eléctrica es el policía más ficiente", y que se ha convertido en la imagen más conocida que asocia la transparencia y la lucha contra la corrupción. Accesible en https://archive.org/download/otherpeoplesmone00bran/otherpeoplesmone00bran.pdf

[615] Véase al respecto la Sentencia del Tribunal Constitucional Federal de Alemania, de 15 de diciembre de 1983 Ref. 1 BvR 209/83. Un extracto de la misma se encuentra en Schwabe, J. (2009). *Jurisprudencia del Tribunal Constitucional Federal Alemán.* Berlín: Konrad-Adenauer-Stiftung e V. pp 95-102. Recuperado en http://www.kas.de/wf/doc/kas_16817-544-4-30.pdf. Un estudio sobre la misma, se encuentra en Heredero Higueras, M. (1983). La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población**.** *Documentación Administrativa, 198, pp 139-159*. Recuperado en https://revistasonline.inap.es/index.php?journal=DA&page=article&op=download&path%5B%5D=4687&path%5B%5D=4741

Lo primero que hay que destacar es que, a diferencia de lo sucedido en el pasado —en el que las normas de acceso a la información y las de protección de datos no contenían ninguna regulación que las conectase—, en la LTBG sí se establecen unas reglas específicas para articular la relación entre ambos derechos. Reconoce RODRÍGUEZ ÁLVAREZ que esto no significa que el ordenamiento español desconociera el principio de publicidad de los actos de los poderes públicos, ni que no tuviéramos reconocido ningún derecho de acceso a la información en manos de los órganos públicos. Lo que faltaba en España era una regulación general, de carácter transversal, de la transparencia de la actuación de los poderes públicos y un reconocimiento igualmente general del derecho de acceso a la información, sin necesidad de acreditar interés específico, ni motivar la petición[616].

Pues bien, la relación entre ambos derechos, de acceso a la información y a la intimidad y a la protección de datos, es potencialmente conflictiva. Sin embargo, convergen en un punto de conexión, la divulgación por las autoridades públicas de información que contiene datos personales, lo que requiere dilucidar cuál es la normativa aplicable y las determinaciones que permitan maximizar la eficacia de ambos derechos. Y, además, hacerlo de forma adaptada al mundo digital en que vivimos, en el que la expansión de la informática, con su capacidad para almacenar contenidos de forma ilimitada, cruzar informaciones y divulgarlas, precisan de soluciones jurídicas adaptada a esta realidad. Los ciudadanos están en contra de un "Gran Hermano" que les impida conservar un reducto de reserva que les garantice la libre determinación personal al margen de miradas ajenas, pero también existe en la actualidad una opinión general acerca de la necesidad de transparencia en la gestión pública, que no utilice como excusa el argumento de la protección de datos para impedir que se sepan y conozcan detalles

[616] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, p. 55.

tales como quién ejerce la autoridad pública, cómo la ejerce y en qué se gastan los fondos públicos, etc.

De ahí que con frecuencia se hayan presentado como derechos antagónicos, y que entre algunos defensores de la transparencia se pueda apreciar incluso cierta animadversión hacia la protección de datos por considerar que constituye un impedimento que dificulta o impide el acceso a la información y que, en general, se erige como un obstáculo a la transparencia. Es cierto que esta hostilidad responde, en parte, a experiencias reales, pues en nuestro país se ha utilizado durante mucho tiempo la protección de datos como excusa para denegar indebidamente el acceso o la publicación de informes de interés público. Pero que se hayan evidenciado usos indebidos o, incluso, abusos de un derecho no debería llevar a cuestionar se reconocimiento, sino a establecer los límites y las garantías apropiadas para evitar usos abusivos o espurios del mismo.

En este sentido, la vigencia, junto a la normativa de protección de datos, de una regulación general de la transparencia y del derecho de acceso a la información debiera contribuir de manera decisiva a mitigar la invocación inapropiada de la protección de datos personales para denegar el acceso a informaciones de interés público. A partir de ahora, será necesario justificar las resoluciones denegatorias conforme a lo previsto en el artículo 20.2 LTBG, según el cual, «serán motivadas las resoluciones que denieguen el acceso, las que concedan el acceso parcial o a través de una modalidad distinta a la solicitada y las que permitan el acceso cuando haya oposición de un tercero». Y, en todo caso, la argumentación con la que se sustentes las denegaciones será susceptible de ser impugnada y revisada a través de recursos administrativos y judiciales.

No procede conceder invariablemente un mayor valor a la protección de los derechos de los afectados, ni es admisible otorgar una primacía automática al objetivo de la transparencia frente al derecho a la protección de datos. La lógica de los derechos llama a la ponderación y exige procedimientos y garantías para hacerlos efectivos. Se trata de apuntar soluciones. Soluciones en las que el derecho y lo que se ha llamado el «código» han de ir de la mano, siendo tarea nuestra la de garantizar que no sea el «código»

en que condicione el alcance de los derechos, sino el que deba adaptarse a las decisiones políticas jurídicamente estructuradas[617]. Debe ser el derecho el que ofrezca o aporte soluciones. No debe quedar a una especie de "determinismo" digital y a la libre apreciación de cada responsable. Hay que tratar de ofrecer al legislador, a los aplicadores del derecho y a la sociedad posibles soluciones fundadas en criterios sólidos en pro de la seguridad jurídica[618].

1.2 El derecho a la protección de datos como límite a la transparencia

Resulta imprescindible aclarar la relación existente entre transparencia y protección de datos, sobre todo teniendo en cuenta que la transparencia es capital para el desarrollo de una sociedad abierta y democrática, y que el respeto a la protección de datos no debe considerarse un obstáculo al derecho de acceso a la información.

Ahora bien, no debemos olvidar que una de las excepciones que pueden invocarse al ejercer el derecho de acceso es la derivada de la protección de datos, o de la existencia de información o documentos que afecten a la intimidad de las personas, así como de información que afecte a la seguridad ciudadana. Ni la transparencia ni la protección de datos son absolutos. Es imprescindible conseguir un equilibrio entre ambos derechos.

La transparencia ya no solo opera como un terreno limitado o restringido con respecto al derecho a la protección de datos personales, sino que se ha configurado asimismo como un derecho prestacional que requiere una

---

[617] Lessig L. (2001). El código y otras leyes del ciberespacio, Madrid: Taurus. y Lessig L. (2009). Código 2.0. Madrid: Traficantes de sueños.

[618] Guichot Reina. E. (2012). Transparencia versus Protección de Datos. En Blasco Esteve A. (Coord) *El Derecho Público de la crisis económica. Transparencia y Sector Público. Hacia un nuevo Derecho Administrativo*. Madrid: INAP, p. 288.

actuación positiva por parte de las autoridades públicas, precisamente en el ejercicio del derecho a la protección de datos[619].

En otras palabras, la transparencia podría considerarse una especie de "subderecho"[620] de los comprendidos en el derecho a una buena administración[621] y en el derecho de acceso a los documentos[622], reconocidos en la Carta de los Derechos Fundamentales de la Unión Europea[623]. Podemos afirmar que aquella constituye, sin ningún género de dudas, una demanda actual de la sociedad.

---

[619] Tomás Mallén, B. (2015). Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo Derecho europeo de protección de datos*. Valencia: Tirant lo Blanch.

[620] Véase al respecto Tomás Mallén, B. (2004) *El derecho fundamental a una buena administración*. Madrid: INAP.

[621]La Carta de los Derechos Fundamentales de la Unión Europea (DOCE 2000/C 364/01 18/12/2000) dispone en su artículo 41 en relación al Derecho a una buena administración, que «1. Toda persona tiene derecho a que las instituciones y órganos de la Unión traten sus asuntos imparcial y equitativamente y dentro de un plazo razonable. 2. Este derecho incluye en particular: - el derecho de toda persona a ser oída antes de que se tome en contra suya una medida individual que le afecte desfavorablemente, - el derecho de toda persona a acceder al expediente que le afecte, dentro del respeto de los intereses legítimos de la confidencialidad y del secreto profesional y comercial, - la obligación que incumbe a la administración de motivar sus decisiones. 3. Toda persona tiene derecho a la reparación por la Comunidad de los daños causados por sus instituciones o sus agentes en el ejercicio de sus funciones, de conformidad con los principios generales comunes a los Derechos de los Estados miembros. 4. Toda persona podrá dirigirse a las instituciones de la Unión en una de las lenguas de los Tratados y deberá recibir una contestación en esa misma lengua».

[622] El artículo 42 de la Carta de los Derechos Fundamentales reconoce expresamente el Derecho de acceso a los documentos en los siguientes términos «todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro tiene derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión».

[623] En relación a la Carta de los Derechos Fundamentales de la Unión Europea, el documento «El respeto de los derechos fundamentales en la Unión Europea» declara expresamente que los derechos que en ella se recogen no son nuevos: la Carta se basa en el «Derecho establecido», es decir, refunde en un mismo documento los derechos fundamentales reconocidos por los Tratados comunitarios, los principios constitucionales comunes de los Estados miembros, el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales y las Cartas Sociales de la UE y del Consejo de Europa. No obstante, el texto de la Carta presta especial atención a los problemas planteados por la situación actual y la evolución futura en campos como la tecnología de la información o la ingeniería genética al establecer derechos como la protección de los datos personales o los derechos asociados a la bioética. También responde a la demanda actual de transparencia e

Se ha señalado anteriormente la opinión del Grupo de Trabajo del artículo 29 en relación al carácter público de un dato de carácter personal. Resulta necesario conciliar el respeto del derecho a la intimidad y a la protección de los datos personales de los ciudadanos con el derecho a acceder a la información del sector público, y en este sentido aquel concluye[624] que es necesario tener en cuenta los siguientes aspectos:

Valoración caso por caso de la cuestión de si un dato de carácter personal puede publicarse/hacerse accesible o no, y en caso afirmativo en qué condiciones y en qué soporte (digitalización o no, difusión en internet o no, etc.).
Principios de finalidad y legitimidad.
Información de la persona en cuestión.
Derecho de oposición de la persona en cuestión; utilización de las nuevas tecnologías para contribuir al respeto del derecho a la intimidad.

También es importante en este aspecto la jurisprudencia europea, ya abundante. Me centraré en la sentencia del Tribunal de Justicia de 20 de mayo de 2003, Rundfunk y otros, Asuntos C- 465/00, C-138/01 y C-139/01, y en la sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager[625] contra Comisión, Asunto T-194/04, y la sentencia

---

imparcialidad en el funcionamiento de la administración de la Unión, incorporando el derecho a una buena administración y el derecho de acceso a los documentos administrativos de las instituciones, sobre la base de los elementos fundamentales de la jurisprudencia del Tribunal de Justicia en este ámbito. El contenido de las *Fichas técnicas sobre la Unión Europea*, Parlamento Europeo, diciembre 2016, http://www.europarl.europa.eu/atyourservice/es/displayFtu.html?ftuId=FTU_2.1.2.html

624 Véase el Dictamen 3/99 del Grupo de Trabajo del Artículo 29, relativo a Información del sector público y protección de datos personales. Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado "La información del sector público: un recurso clave para Europa" COM(1998) 585, WP20, de 3 de mayo de 1999.

625 La Sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager contra Comisión, Asunto T-194/04. juzga si era pertinente facilitar a terceros interesados los datos de las personas que intervinieron en una reunión de trabajo de la Comisión. El Tribunal parte de la base de que la lista de los participantes en la reunión que figuran en el acta de la misma contiene datos personales. Pero a partir de aquí lleva a cabo una serie de consideraciones que desembocan en la decisión de que tales datos deben ser facilitados cuando se lleva a cabo una solicitud de acceso a la información basándose en el Reglamento 1049/2001. El apartado 123 de la Sentencia declara que «el

del Tribunal de Justicia de 29 de junio de 2010, Comisión[626] contra Bavarian Lager, Asunto C-28/08 P.

El primero de los principios relativos al tratamiento de datos personales consignado en el RGPD es la transparencia, junto con la licitud y la lealtad, de modo que los datos serán[627]

> *«tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)»*

---

mero hecho de que un documento contenga datos personales no significa necesariamente que se ponga en peligro la intimidad o la integridad de las personas de que se trata, a pesar de que la actividad profesional no esté, en principio, excluida del concepto de 'vida privada' en el sentido del artículo 8 del CEDH». En particular, contener los nombres de los representantes de las entidades que participaron en la reunión no pone en peligro la intimidad de las personas, pues éstas actúan en representación de sus entidades y las opiniones vertidas en la reunión no contienen opiniones individuales, sino posturas imputables a las entidades. El Tribunal concluye en su apartado 132 que «la divulgación de los nombres en cuestión no da lugar a una injerencia en la intimidad de las personas que participaron en la reunión y no supone un perjuicio para la protección de su intimidad y de la integridad de sus personas», por lo que tales datos pueden y deben ser facilitados a quien lo solicitó.

[626] Sentencia del Tribunal de Justicia de la Unión Europea de 29 de junio de 2010, asunto C-28/08 P, Comisión contra Bavarian Lager. El Tribunal resolvió el recurso de casación interpuesto por la Comisión Europea por el que se solicitaba la anulación de la Sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007 que había anulado la Decisión de la Comisión de 18 de marzo de 2004 desestimatoria de una solicitud de Bavarian Lager para acceder al acta completa de la reunión oficial celebrada el 11 de octubre de 1996 en el marco de un procedimiento de incumplimiento. El TJUE concluyó que, según el régimen anterior de la Directiva 95/46/CE y los Reglamentos nº 45/2001 y nº 1049/2001, la Comisión actuó legítimamente al verificar si las personas afectadas habían otorgado su consentimiento para la difusión de los datos personales que les concernían y cumplió suficientemente con su obligación de transparencia al difundir una versión del acta expurgando cinco nombres de participantes en la reunión. Además, al exigir que para las cinco personas que no otorgaron su consentimiento expreso se demostrara la necesidad de transmitir esos datos personales, la Comisión se ajustó al artículo 8 b) del Reglamento nº 45/2001«Artículo 8 Transmisión de datos personales a destinatarios, distintos de las instituciones y los organismos comunitarios, sujetos a la Directiva 95/46/CE. […] los datos personales sólo se transmitirán a destinatarios sujetos al Derecho nacional adoptado para la aplicación de la Directiva 95/46/CE, cuando: […] b) el destinatario demuestre la necesidad de que se le transmitan los datos y no existan motivos para suponer que ello pudiera perjudicar los intereses legítimos del interesado» y, al no haberse presentado ninguna justificación expresa y legítima ni ningún argumento convincente para demostrar la necesidad de la transmisión de dichos datos personales, la Comisión ni pudo ponderar los distintos intereses de las partes implicadas ni verificar si no existían motivos para suponer que esa transmisión podría perjudicar los intereses legítimos de los interesados.

[627] Véase la letra a) del apartado 1 del artículo 5 RGPD.

Anteriormente hicimos referencia al Considerando 154 RGPD cuando advierte que al aplicarlo, se debe tener en cuenta el principio de acceso del público a los documentos oficiales, ya que puede considerarse de interés público. En idéntica línea, el artículo 24.1 del mismo texto legal obliga al responsable del tratamiento a aplicar medidas técnicas y organizativas apropiadas «a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento».

Se persigue conciliar esos derechos personales de los interesados con la consecuencia de la libertad de empresa[628].

---

[628] Puede argumentarse, en tal sentido, que dicha conciliación viene de «la proporcionalidad como ponderación equilibrada entre la transparencia pública y la protección de datos», como bien ha comentado, con relación al caso Volker un Markus Schecke y Eifert (C-92/09 y C-93/09, Sentencia de 29 de noviembre de 2010), Rallo Lombarte, A. (2014). *El derecho al olvido en Internet. España contra Google*, Madrid: Centro de Estudios Políticos y Constitucionales, pp. 231-233. Este supuesto resuelve las cuestiones prejudiciales planteadas a raíz de los litigios en los que Volker und Markus Schecke GbR y el Sr. Eifert se oponían a que el Land de Hesse publicase en el sitio web de la Agencia Federal de Agricultura y Alimentación sus datos personales como beneficiarios de fondos económicos de ayuda agrícola. En su sentencia, Tribunal declara que el derecho a la protección de datos de la Carta de Derechos Fundamentales de la Unión Europea no constituye una prerrogativa absoluta, sino que debe ser considerado en relación con su función en la sociedad, pudiendo introducirse limitaciones a su ejercicio que estén establecidas por la ley, respeten su contenido esencial y el principio de proporcionalidad, sean necesarias y respondan efectivamente a objetivos de interés general reconocidos por la Unión o a la necesidad de protección de los derechos y libertades de los demás. El Tribunal entiende que la injerencia resultante de la publicación en un sitio web de los datos nominales de los beneficiarios de las ayudas comunitarias debía considerarse una injerencia establecida por la ley, que perseguía el objetivo de interés general reconocido por la Unión de aumentar la transparencia y control sobre la utilización de fondos comunitarios, y que la limitación de los derechos de los artículos 7 y 8 de la Carta de Derechos Fundamentales de la Unión Europea resultaba proporcionada a la finalidad legítima perseguida. Por otro lado, el TJUE sostuvo en su Considerando 85 que «no cabe atribuir una primacía automática al objetivo de transparencia frente al derecho a la protección de los datos de carácter personal (véase en este sentido la sentencia Comisión/Bavarian Lager, apartados 75 a 79), ni siquiera, aunque estén en juego intereses económicos importantes»; y añade en el Considerando 86 que «dado que las excepciones a la protección de los datos de carácter personal y las limitaciones de dicha protección deben establecerse sin sobrepasar los límites de lo estrictamente necesario (sentencia Satakunnan Markkinapörssi y Satamedia, apartado 56) y que cabe concebir medidas que entrañen lesiones de menor gravedad a este derecho fundamental de las personas físicas, sin dejar por ello de contribuir eficazmente al logro de los objetivos de la normativa de la Unión controvertida, procede concluir que el Consejo y la Comisión han sobrepasado los límites que impone el respeto del principio de proporcionalidad al obligar a publicar los nombres de todas las personas físicas beneficiarias de ayudas del FEAGA y del Feader y los importes específicos percibidos por ellas».

1.3 El potencial conflicto: dos derechos de rango constitucional y desarrollo legal con un punto de conexión, la divulgación por las autoridades públicas de información que contiene datos personales.

1.3.1 El derecho de acceso a la información pública

A nivel global, existen dos aproximaciones básicas. Por una parte, la que considera que el derecho de acceso a la información se integra en la libertad de información, que comporta, de este modo, la consiguiente obligación de las autoridades públicas de facilitarla, superando así la concepción meramente «abstencionista» del derecho entendido como proscripción de las injerencias públicas. A esta solución se ha llegado, por lo general, en aquellas Constituciones y sistemas iusfundamentales menos recientes. Por otra, la que estima que se trata de un derecho fundamental autónomo, característica de las Constituciones y los textos iusfundamentales más modernos.

A la primera de estas aproximaciones, la de la integración del derecho de acceso a la información en la libertad de información, se ha llegado recientemente en la aplicación de los instrumentos internacionales de protección de los derechos humanos, que no reconocieron autónomamente el derecho de acceso a la información pública. En el sistema del Convenio Europeos para la Protección de los Derechos Humanos y de las Libertades Fundamentales (en adelante, CEDH), y a falta de la consagración expresa en su articulado del derecho a la información en poder de la Administración se ha planteado si este derecho debe considerarse incluido en su artículo 10[629], que se refiere a la libertad expresión, que comprende la liberta de

---

[629] El artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales expresamente reconoce: «1. Toda persona tiene derecho a la libertad de expresión. Este derecho comprende la libertad de opinión y la libertad de recibir o de comunicar informaciones o ideas sin que pueda haber injerencia de autoridades públicas y sin consideración de fronteras. El presente artículo no impide que los Estados sometan a las empresas de radiodifusión, de cinematografía o de televisión a un régimen de autorización previa. 2. El ejercicio de estas libertades, que entrañan deberes y responsabilidades, podrá ser sometido a ciertas formalidades, condiciones, restricciones o sanciones, previstas por la ley, que constituyan medidas necesarias, en una sociedad

recibir o de comunicar informaciones o ideas sin que pueda hacer interferencias de la autoridad pública. Hasta fechas reciente, la cuestión se había planteado frontalmente ante el Tribunal Europeo de Derechos Humanos (en adelante, TEDH) en contadas ocasiones, y en todos los casos, el Tribunal había enfocado la demanda por la vía de la posible vulneración del artículo 8[630] del mismo, que garantiza el respeto a la vida privada y familiar, al domicilio y a la correspondencia. Esta solución se explica porque en estos asuntos se pretendía información concerniente a la vida personal de los propios solicitantes, de modo que el TEDH[631] prefirió optar por encajar

---

democrática, para la seguridad nacional, la integridad territorial o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, la protección de la reputación o de los derechos ajenos, para impedir la divulgación de informaciones confidenciales o para garantizar la autoridad y la imparcialidad del poder judicial».

630 El artículo 8 del CEDH se refiere al derecho al respeto a la vida privada y familiar, y afirma que «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

631 El tratamiento de información relativa a la vida privada de un individuo recae en el ámbito del artículo 8.1 CEDH. Así lo expresa el TEDH en la Sentencia Leander c. Suecia, de 26 de marzo de 1987, serie A nº 116 § 48. Esta sentencia tiene como origen la solicitud del señor Leander al no haber podido ocupar un puesto de trabajo debido a la existencia de una serie de antecedentes policiales y políticos en el Registro de la Policía. Estos datos hicieron que se le catalogara como peligroso para la seguridad, y se le excluyera del empleo. El Tribunal señala que el registro secreto de la policía contenía datos relativos a la vida privada del señor Leander, y así, tanto su almacenamiento como su comunicación, unidos a la negativa de permitirle que los refutara, supuso una violación del derecho al respeto de su vidad privada, garantizado por el artículo 8.1. CEDH. En idéntico sentido véanse las Sentencias Amann c. Suiza, de 16 de febrero de 2000 § 69 y 80, y Rotaru c. Rumanía, de 4 de mayo de 2000 § 43 y 46. En 1946, tras el establecimiento del régimen comunista, el Sr. Rotaru vio denegada una solicitud para publicar dos folletos que las autoridades entendieron que expresaban sentimientos antigubernamentales. Tras remitir sendas cartas protestando por la supresión de la libertad de expresión, fue detenido en 1948 y condenado por injurias a un año de prisión. En 1989, tras la caída del régimen comunista, el Decreto 118/1990 otorgó ciertos derechos a los perseguidos por el régimen comunista que no hubieran participado en actividades fascistas y el Sr. Rotaru obtuvo una indemnización por el año de prisión. Pero, durante el procedimiento judicial, el Ministerio del Internet presentó una carta del Servicio de Inteligencia Rumano en la que se afirmaba que, durante sus estudios universitarios, el Sr. Rotaru fue miembro de una Asociación de Estudiantes Cristianos, que pertenecía a la sección juvenil del Partido Nacional Campesino, que ni tenía antecedentes penales ni había sido encarcelado y que había sido interrogado en diversas ocasiones. El demandante interpuso un recurso

la obligación de facilitarla dentro del contenido activo del derecho al respeto a la vida privada, en línea con las facultades positivas que se integran actualmente en el derecho a la protección de datos en los ordenamientos nacionales. En todo caso, el TEDH siempre afirmó que la libertad de recibir información se caracteriza, «al menos de forma principal», como un derecho a obtenerla de los sujetos privados sin injerencia del poder público, si bien se cuidó de no descartar que pudiera hacerse valer frente a la Administración en función de las circunstancias del caso[632]. Aún en fechas recientes, el TEDH afirmó que es difícil derivar del CEDH un derecho general de acceso a la información y a los documentos administrativos[633]. Sin embargo, en el año 2006 el TEDH cambió de criterio jurisprudencial, considerando que el acceso a la información administrativa debía incluirse, *de facto,* en el ámbito objetivo del derecho de acceso a la información pública previsto en el artículo

---

contra el Servicio de Inteligencia Rumano, afirmando que buena parte de dichas informaciones eran falsas y difamatorias y solicitando modificar o destruir el archivo que contenía esa información. Pues bien, frente a las alegaciones de que el artículo 8 CEDH no era aplicable por tratarse de informaciones no relacionadas con la vida privada del demandante, sino con la vida pública, el Tribunal recordó que el almacenamiento de la información relativa a la vida privada de una persona en un registro secreto y su divulgación entraban en el ámbito del artículo 8 CEDH al garantizar el respeto de la vida privada que también comprendería las actividades de carácter profesional o de negocios. La información pública puede entrar en el ámbito de la vida privada si se recoge y se almacena sistemáticamente en archivos en poder de las autoridades. Aunque el Tribunal concluyó que el almacenamiento de información sobre la vida privada tenía una base en la legislación rumana, sentenció que el uso y almacenamiento continuado y la negativa a permitir que la información registrada fuera refutada constituiría una injerencia en el derecho al respeto de la vida privada que no resultaba justificable por falta de conformidad con la ley, ya que este principio exige calidad de las normas jurídicas invocadas en el sentido de suficiente precisión de las circunstancias que ampararían el almacenamiento y uso de la información relativa a la vida privada. El Tribunal estimó una violación del artículo 8 CEDH porque la ley que habilitaba el registro de información personal no resultaba lo suficientemente precisa para preservar las garantías inherentes al derecho a la vida privada como sería, entre otros argumentos, la ausencia de un límite temporal para el almacenamiento de datos personales.

632 El Tribunal en la Sentencia Leander considera que «el derecho a la libertad de recibir información prohíbe básicamente que un Gobierno impida a una persona recibir información que otras quieren o pueden estar dispuestas a ofrecerle. El artículo 10 no confiere al individuo, en circunstancias como las del caso de autos, un derecho de acceso a un registro que contenga información sobre su situación personal, ni conlleva la obligación del Gobierno de facilitar una información tal al individuo». § 74.

633 Véase la Sentencia Tribunal Europeo Derechos Humanos Loiseau c. Francia, de 28 de septiembre de 2004.

10 CEDH, siendo necesario efectuar un estudio de la proporcionalidad entre la injerencia en la libertad de información y la denegación del acceso a la misma[634], y desde el año 2009[635] parece haber asumido ya esta posición, incluyendo una admisión expresa de la evolución de su jurisprudencia al respecto. Así, una denegación de información constituye una injerencia en la libertad de expresión del artículo 10 CEDH. De este modo, el Tribunal asume plenamente su nueva construcción jurisprudencial, y otorga al derecho de acceso la categoría de derecho fundamental amparado en el Convenio. Si bien se trata de asuntos en que los solicitantes de información son sujetos cualificados, el tenor de las sentencias parece apuntar a la generalidad de este enfoque.

Enfoque que, de hecho, coincide con el de los documentos emanados del Consejo de Europa en forma de Recomendaciones, que enlazan de modo expreso el derecho de acceso con la libertad de información consagrada en el artículo 10 CEDH[636], así como con el Convenio 205 del Consejo de Europa sobre acceso a la documentación pública, de 2009, que se remite al artículo 19[637] de la Declaración Universal de Derechos Humanos referido a la libertad de opinión y de expresión.

---

634 Sentencia TEDH Sdruzeni Jihoceské Matky c. República Checa, de 10 de julio de 2006. Se trataba de una solicitud de información sobre el funcionamiento de una central nuclear checa. El TEDH comenzó recordando el sentido original del artículo CEDH, el der reconocer el derecho a obtener una información de los sujetos privados sin injerencia del poder público y afirmó que es difícil deducir del mismo un derecho general de acceso a los datos y documentos administrativos. No obstante, admitió que, en el caso concreto, la denegación de la información constituía una injerencia en el derecho del demandante a recibir información. No obstante, estimó que se trataba de una injerencia no arbitraria sino proporcionada, ya que la solicitud de información versaba sobre aspectos técnicos carentes de interés general y cuyo conocimiento público podía afectar al secreto industrial, a la seguridad nacional y a la salud pública. El TEDH deja apuntado que otra solución cabría en el caso de tratarse de información de interés general sobre el impacto ambiental de la central.

635 Sentencia TEDH Társasag a Szabadságjogokert c. Hungría, de 14 de abril de 2009, y Kennedy c. Hungría, de 16 de agosto de 2009.

636 Así lo hacen la Recomendación del Comité de Ministros de 21 de febrero de 2002, sobre acceso a la información oficial, y la de 13 de julio de 2000, sobre política europea en materia de acceso a archivos.

637 Artículo 19. Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y

Por su parte, la Corte Interamericana de Derechos Humanos ha interpretado que el artículo 13[638] de la Convención Americana sobre Derechos Humanos, referido igualmente a la libertad de pensamiento y de expresión, protege el derecho que tiene toda persona a solicitar el acceso a la información bajo el control del Estado, con las salvedades permitidas bajo el régimen de restricciones de la Convención, en línea con los textos internacionales, y regionales americanos y europeos[639].

---

opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión. Texto accesible en el link http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/spn.pdf

[638] Artículo 13. Libertad de Pensamiento y de Expresión «1. Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección. 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a) el respeto a los derechos o a la reputación de los demás, o b) la protección de la seguridad nacional, el orden público o la salud o la moral públicas. 3. No se puede restringir el derecho de expresión por vías o medios indirectos, tales como el abuso de controles oficiales o particulares de papel para periódicos, de frecuencias radioeléctricas, o de enseres y aparatos usados en la difusión de información o por cualesquiera otros medios encaminados a impedir la comunicación y la circulación de ideas y opiniones. 4. Los espectáculos públicos pueden ser sometidos por la ley a censura previa con el exclusivo objeto de regular el acceso a ellos para la protección moral de la infancia y la adolescencia, sin perjuicio de lo establecido en el inciso 2. 5. Estará prohibida por la ley toda propaganda en favor de la guerra y toda apología del odio nacional, racial o religioso que constituyan incitaciones a la violencia o cualquier otra acción ilegal similar contra cualquier persona o grupo de personas, por ningún motivo, inclusive los de raza, color, religión, idioma u origen nacional». http://www.oas.org/dil/esp/tratados_B-32_Convencion_Americana_sobre_Derechos_Humanos.pdf

[639] Sentencia de la Corte Interamericana de Derechos Humanos, Claude Reyes y otros c. Chile, de 19 de septiembre de 2006. Este caso llega a la Corte Interamericana por la negativa del Estado de brindar al señor Marcel Claude Reyes toda la información que solicitó del Comité de Inversiones Extranjeras, en relación con la empresa forestal Trillium y el Proyecto Río Condor, el cual era un proyecto de deforestación que él consideraba podía ser perjudicial para el medio ambiente e impedir el desarrollo sostenible de Chile. El Estado, en sede internacional, argumenta que no se entregó la información financiera de la empresa porque ésta podría afectar el interés colectivo, inhibir las inversiones y afectar la competencia de la empresa en el mercado, aduciendo además que no era el titular de dicha información y no podía entregar información de terceros que se encontrase en su poder. La Corte Interamericana sanciona al Estado Chileno por la negativa de brindar información, considerando que ésta es de interés público, y por la falta de un recurso judicial efectivo para salvaguardar el derecho de acceso a la información. La Corte Interamericana determina cuál es el contenido del derecho de acceso a la información pública y su marco normativo internacional, destacando la importancia de este derecho y estableciendo que cualquier restricción al mismo debe ser necesaria en la sociedad

En relación a la segunda de las aproximaciones, destacar que en las Constituciones más recientemente promulgadas o reformadas, se tiende al reconocimiento autónomo del derecho de acceso respecto de la libertad de información. Así, en el Derecho comunitario, se encuentra reconocido como derecho fundamental autónomo relacionado con la ciudadanía[640] en la Carta de los Derechos Fundamentales de la Unión Europea[641]. De igual modo, el Tratado de Funcionamiento de la Unión Europea[642], además de dotar de rango constitucional a la Carta Europea de Derechos Fundamentales, reconoce en su articulado el derecho de acceso[643].

---

democrática y debe respetar el principio de legalidad. La sentencia se encuentra accesible en http://www.corteidh.or.cr/docs/casos/articulos/seriec_151_esp.pdf

[640] Artículo 42. Todo ciudadano de la Unión o toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos del Parlamento Europeo, del Consejo y de la Comisión.

[641] Carta de los Derechos Fundamentales de la Unión Europea (2000/C 364/01) http://www.europarl.europa.eu/charter/pdf/text_es.pdf

[642] Conocido como Tratado de Lisboa, en vigor desde el 1 de diciembre de 2009. La versión consolidada del Tratado (2012/C 326/47), puede consultarse en el siguiente link http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:12012E/TXT&from=ES

[643] El artículo 15.3 (antiguo artículo 255 TCE) del Tratado de Funcionamiento de la Unión Europea declara que: «Todo ciudadano de la Unión, así como toda persona física o jurídica que resida o tenga su domicilio social en un Estado miembro, tendrá derecho a acceder a los documentos de las instituciones, órganos y organismos de la Unión, cualquiera que sea su soporte, con arreglo a los principios y las condiciones que se establecerán de conformidad con el presente apartado. El Parlamento Europeo y Consejo, con arreglo al procedimiento legislativo ordinario, determinarán mediante reglamentos los principios generales y los límites, por motivos de interés público o privado, que regulan el ejercicio de este derecho de acceso a los documentos. Cada una de las instituciones, órganos u organismos garantizará la transparencia de sus trabajos y elaborará en su reglamento interno disposiciones específicas sobre el acceso a sus documentos, de conformidad con los reglamentos contemplados en el párrafo segundo. El Tribunal de Justicia de la Unión Europea, el Banco Central Europeo y el Banco Europeo de Inversiones sólo estarán sujetos al presente apartado cuando ejerzan funciones administrativas. El Parlamento Europeo y el Consejo garantizarán la publicidad de los documentos relativos a los procedimientos legislativos en las condiciones establecidas por los reglamentos contemplados en el párrafo segundo».

Reconoce GUICHOT REINA[644] que en el Derecho de los Estados de la Unión Europea es mayoritario el reconocimiento constitucional explícito del derecho del derecho de acceso a la información pública como derecho autónomo[645]; y lo mismo ocurre en los Estados americanos[646].

En España también se recoge el derecho de acceso[647] en la Constitución española. Sin embargo, el artículo 105 no se inserta en el Título I «De los derechos y deberes fundamentales», sino en el Título IV («Del Gobierno y de la administración»), lo que ha dado lugar a una polémica doctrinal en torno a si se trata de un derecho autónomo[648] o, por el contrario, de una manifestación de la libertad de información[649]. La jurisprudencia del Tribunal

---

[644] Guichot Reina. E. (2012). Transparencia versus Protección de Datos. En Blasco Esteve A. (Coord) El Derecho Público de la crisis económica. Transparencia y Sector Público. Hacia un nuevo Derecho Administrativo. Madrid: INAP, p. 294.

[645] En el examen por parte de Kranenborg, H.y Voermans, W. (2005). Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation. Países Bajos: Europa Law Publishing, p. 11, catorce de los veinticuatro países de la Unión con Constitución lo han incluido en ellas.

[646] Mientras que en los sistemas canadiense y estadounidense se discute si puede extraerse de la libertad de información, a falta de un reconocimiento autónomo, en los Estados latinoamericanos con Constituciones o reformas constitucionales reciente, la acogida del derecho de acceso como derecho fundamental autónomo es mayoritaria.

[647] Artículo 105. b) El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas.

[648] En esta línea se inscribirían, entre otros, Álvarez Rico, M. (1979). El derecho de acceso a los documentos administrativos. *Documentación Administrativa, 183*, *pp. 103-133* o Pomed Sánchez, L. A. (1989). *El acceso de los ciudadanos a los archivos y registros administrativos*, Madrid: INAP. Parcialmente en sintonía Mestre Delgado, J.F. (1993). *El derecho de acceso a archivos y registros administrativos [análisis del artículo 105.b) de la Constitución]*. Madrid: Civitas, para quien el derecho de acceso es un instrumento para la efectividad de otros derechos, como la protección de la intimidad (respecto al acceso por el propio interesado a sus datos), la tutela judicial efectiva, o la libertad de información (en cuanto al acceso de los medios de comunicación a la información oficial).

[649] Es la tesis de Villaverde Menéndez, I (1995). *Los derechos del público*. Madrid: Tecnos, p. 118, seguida y matizada por Fernández Ramos, S (1997). *El derecho de acceso a los documentos administrativos*. Madrid: Marcial Pons, pp. 350-358.

Supremo se declara partidaria de una interpretación conjunta de los artículos 20.1.d) y 105.b) CE[650]

Es cierto que estamos ante un debate teórico, una vez alcanzado el consenso, a nivel mundial, de que se trata de un derecho fundamental, bien mediante su integración en la liberta de información o bien mediante su afirmación como derecho autónomo, allá donde los sistemas constitucionales más modernos lo han previsto. Se trata de derechos, como mínimo, íntimamente conectados[651].

---

[650] En palabras del Tribunal Supremo en jurisprudencia reiterada por todas, la Sentencia de 19 de mayo de 2003 establece expresamente: «El artículo 105 b) de la Constitución dispone que la ley regulará, entre otras materias, «El acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas». Este precepto constitucional remite expresamente a la configuración legal el ejercicio del derecho de acceso a los archivos y registros administrativos, como derecho no fundamental, aunque relacionado con el derecho de participación política, con el de libertad de información y con el de tutela judicial efectiva. Refleja una concepción de la información que obra en manos del poder público acorde con los principios inherentes al Estado democrático (en cuanto el acceso a los archivos y registros públicos implica una potestad de participación del ciudadano y facilita el ejercicio de la crítica del poder) y al Estado de derecho (en cuanto dicho acceso constituye un procedimiento indirecto de fiscalizar la sumisión de la Administración a la ley y de permitir con más eficacia el control de su actuación por la jurisdicción contencioso-administrativa).” Cuando se le ha planteado frontalmente la relación entre los artículos 20.1.d) y 105.b) de la Constitución, en un caso paradigmático de demanda de información formulada por un profesional de los medios de comunicación en relación a una investigación periodística sobre el destino de los fondos públicos, ha concedido que el derecho a comprobar la veracidad de la información mediante el acceso a la misma deriva del artículo 20.1.d), pero ha de conectarse con el artículo 105.b). Es necesaria una interpretación conjunta del ordenamiento, que lleva a resolver la cuestión aplicando la normativa legal sobre acceso, esto es, a día de hoy, el artículo 37 de la LRJPAC».

[651] Reflejo de ello, puede verse en Piñar Mañas, J. L. (2010). Transparencia y protección de datos: las claves de un equilibrio necesario. En Ruiz Ojeda, A. L. (Coord.), *El gobierno local. Estudios en homenaje al profesor Luis Morell Ocaña*, Madrid: Iustel, pp. 1023-1044, p. 1041: «En efecto, la transparencia, además de ser en sí un derecho fundamental autónomo (artículo 105), es requisito imprescindible para la efectividad del derecho de participación que reconocen los artículos 9 y 23. Lo es también para el ejercicio del derecho a la libertad de expresión y de información (artículo 20) y se trata de un derecho fundamental que debe ser interpretado de acuerdo a los tratados y acuerdos internacionales sobre la materia, así como la jurisprudencia de los Tribunales que los apliquen (artículo 10.2)».

1.3.2 Derecho a la protección de datos

Ya es un lugar común señalar que estamos viviendo un momento en el que, fundamentalmente como consecuencia de la aplicación de las nuevas tecnologías, es posible recabar ingentes cantidades de datos sobre cualquier persona y obtener información a veces vital sobre ella y su entorno.

Se ha llegado a decir que carecemos de privacidad y que hemos de resignarnos con ello[652] o que si hoy disponemos de intimidad es porque alguien tolera que la tengamos.

Sin embargo, el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea reconoce expresamente el derecho fundamental a la protección de datos de carácter personal del siguiente modo:

> *«1. Toda persona tiene derecho a la protección de los datos de carácter personal que le conciernen. 2. Estos datos se tratarán de modo leal, para fines concretos y sobre la base del consentimiento de la persona afectada o en virtud de otro fundamento legítimo previsto por la Ley. Toda persona tiene derecho a acceder a los datos recogidos que le conciernan y a obtener su rectificación. 3. El respeto de estas normas quedará sujeto al control de una autoridad independiente».*

Tal precepto supone el punto de partida de una nueva etapa en la protección de datos de carácter personal, reconocida ya como derecho fundamental, autónomo e independiente del derecho a la intimidad. Punto de partida que arranca precisamente en el ámbito europeo, en el año 2000, con el ya citado artículo 8 de la Carta Europea de Derechos Fundamentales adoptada en Niza en mayo de ese año y, además, con diversas sentencias del Tribunal

---

[652] La revista Wired recogía en el año 1999 las declaraciones de Scott McNEaly, quien en su calidad de chief executive officer CEO de Sun Microsystems, afirmó expresamente que «Consumer privacy issues are a "red herring". You have zero Privacy anyway. Get over it». La traducción no literal viene a significar que «Las cuestiones de privacidad del consumidor son una cortina de humo. No tienes privacidad de todos modos. Supéralo» El contenido de la revista se puede consultar en http://archive.wired.com/politics/law/news/1999/01/17538

Europeo de Derechos Humanos, en particular las dictadas en los asuntos Amann contra Suiza, de 16 de febrero de 2000 y Rotaru contra Rumania, de 4 de mayo de 2000. Anteriormente nos hemos referido a ellas.

En España la consideración de la protección de datos como un derecho autónomo e independiente ha sido consolidada por el Tribunal Constitucional en su conocida Sentencia 292/2000, de 30 de noviembre, de la que debemos recordar el fundamento jurídico 7º:

> *«El contenido del Derecho fundamental a la protección de datos consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso. Estos poderes de disposición y control sobre los datos personales, que constituyen parte del contenido del Derecho fundamental a la protección de datos se concretan jurídicamente en la facultad de consentir la recogida, la obtención y el acceso a los datos personales, su posterior almacenamiento y tratamiento, así como su uso o usos posibles, por un tercero, sea el Estado o un particular. Y ese derecho a consentir el conocimiento y el tratamiento, informático o no, de los datos personales, requiere como complementos indispensables, por un lado, la facultad de saber en todo momento quién dispone de esos datos personales y a qué uso los está sometiendo, y, por otro lado, el poder oponerse a esa posesión y usos. En fin, son elementos característicos de la definición constitucional del Derecho fundamental a la protección de datos personales, los derechos del afectado a consentir sobre la recogida y uso de sus datos personales y a saber de los mismos. Y resultan indispensables para hacer efectivo ese contenido el reconocimiento del derecho a ser informado de quién posee sus datos personales y con qué fin, y el derecho a poder oponerse a esa posesión y uso requiriendo a quien corresponda que ponga fin a la posesión y empleo de los datos. Es*

decir, exigiendo del titular del fichero que le informe de qué datos posee sobre su persona, accediendo a sus oportunos registros y asientos, y qué destino han tenido, lo que alcanza también a posibles cesionarios; y, en su caso, requerirle para que los rectifique o los cancele».

Ante todo, es capital la consideración del derecho a la protección de datos como autónomo, diferenciado de los de privacidad e intimidad. Un derecho que, y éste es el elemento estructural del mismo, atribuye a su titular un poder de disposición sobre sus propios datos personales, sean o no íntimos.

Pasa así a un segundo plano la discusión acerca de qué se entiende por privacidad o intimidad, pues el núcleo protector del derecho, como acabo de resaltar, se extiende a todo tipo de datos, sin perjuicio, obviamente, de que unos, por su especial naturaleza, requieran de mayor protección que otros. Este sería el caso de los llamados datos sensibles o especialmente protegidos (a los que se refiere el artículo 7 de la LOPD).

Esa consideración del derecho fundamental a la protección de datos explica y justifica el contenido de los principios que configuran su núcleo esencial. Tales principios, cuya violación o desconocimiento implica la violación o desconocimiento del derecho, pueden reconducirse a los siguientes: consentimiento, información, finalidad, calidad de los datos, con especial referencia a la proporcionalidad, seguridad y control independiente. Principios a los que pueden añadirse los de utilización leal de los datos y minimización en el uso de los mismos, éste último reconducible también, en mi opinión, al de proporcionalidad. Principios que para ser efectivos requieren el reconocimiento, garantía y tutela de los derechos de acceso, rectificación, cancelación y oposición[653].

En los sistemas iusfundamentales más "antiguos", que no aluden al derecho a la protección de datos, el derecho a la protección de datos se ha hecho

---

[653] Piñar Mañas J.L. (2005). El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. *Asamblea: Revista Parlamentaria de la Asamblea de Madrid, 13*, págs. 21 y ss.

derivar, por lo común[654], de la protecció de la "vida privada" o "intimidad". Se ha planteado si la recogida, almacenamiento y comunicación por terceros de información personal, y las facultades del interesado de acceso, rectificación y cancelación de dicha información se incluyen en el derecho al respeto a la vida privada[655] y familiar consagrado en el artículo 8 del CEDH. La respuesta ha sido positiva[656]. El TEDH ha entendido que dicho artículo impone obligaciones negativas de no injerencia, por ejemplo, no recabar ni almacenar datos personales sin consentimiento del interesado, y también positivas, como por ejemplo, a la Administración, el facilitar información sobre los datos personales del afectado que se hallen en su poder[657]. En

---

[654] Aunque con excepciones, como el caso alemán, en el que, como el propio derecho a la intimidad, se deriva del derecho a la dignidad humana y al libre desarrollo de la personalidad. Véase la Ssentencia del Tribunal Constitucional Federal de 15 de diciembre de 1983, comentada con antelación.

[655] El TEDH ha dado el ma amplio sentido al término "vida privada", de tal modo que ha afirmado que entran en el campo de protección del artículo 8 CEDH la recogida, almacenamiento o difusión de datos personales relativos a actividades profesionales o económicas, ya que la vida privada no se limita a un círculo íntimo, sino que debe englobar, en cierta medida, el derecho a desarrollar sus relaciones con sus semejantes, y no hay ninguna razón de principio para excluir las actividades profesionales o comerciales de la noción de vida privada en la medida en que es en el trabajo donde la mayoría de las personas tienen las mayores ocasiones de estrechar sus lazos con el mundo exterior, de tal forma que no es necesario que se trate de informaciones «sensibles». Así, en la Sentencia *Amann*, de 16 de febrero de 2000 se deniega a una persona el acceso a una ficha policial con información sobre su actividad profesional. El TEDH estima que la elaboración de la ficha y su conservación carecen de cobertura legal. En la Sentencia de 21 de enero de 1999, *Fressoz y Roire*, una publicación reproduce copias de la declaración de renta del director de una gran multinacional, con ocasión de reivindicaciones laborales de aumento de sueldo de los trabajadores de dicha empresa, copias extraídas delictivamente por un funcionario de Hacienda. El TEDH entiende que ha de prevalecer la libertad de expresión frente al derecho a la intimidad, por el interés social de la noticia y el tratarse de información de fácil acceso al público concerniente a un personaje de relevancia pública.

[656] Entre otras, la inclusión del derecho a la protección de datos en el derecho al respeto a la vida privada protegido por el artículo 8 del CEDH ha sido constatada por el Abogado General Léger en sus conclusiones a la Sentencia del Tribunal de Justicia (Gran Sala) de 30 de mayo de 2006, Parlamento Europeo c. Consejo de la Unión Europea C-317/04 y Comisión de las Comunidades Europeas C-318/04.

[657] En la Sentencia Tribunal Europeo Derechos Humanos Gaskin c. The United Kingdom, de 07 de julio de 1989, se deniega a una persona que fue acogida por los servicios sociales a los informes sobre su pasado. El TEDH estima que en los casos de niños tutelados por los servicios sociales y acogidos por diversas familias, el expediente constituye un sustitutivo de los recuerdos y experiencia de los

relación con los datos personales, se ha considerado que para determinar si ha existido una injerencia no es preciso que se haya producido un uso posterior a su almacenamiento o se haya derivado un perjuicio para su titular.

En los sistemas iusfundamentales más modernos y en las normas reguladoras de la protección de datos, por el contrario, se ha acogido el derecho a la protección de datos como derecho autónomo del derecho a la intimidad. En el Derecho comunitario, el derecho a la protección de datos ha adquirido carta de naturaleza como derecho fundamental autónomo en la Carta de los Derechos Fundamentales, que a su vez se basa en el artículo 286 TCE y en la Directiva 95/46/CE, así como en el artículo 8 del CEDH y en el Convenio del Consejo de Europa de 28 de enero de 1981[658]. En la línea de reconocimiento de un derecho autónomo se inscriben las Constituciones más modernas en el Derecho comparado.

Se ha originado una división en la doctrina española, que reproduce, en realidad, un debate presente en el Derecho comparado, entre los que lo consideran el derecho a la protección de datos un derecho nuevo y autónomo del derecho a la intimidad, y los que ponen de relieve la evolución del derecho a la intimidad que, en la sociedad de la información, y, precisamente por obra de la combinación de la acumulación de información personal y medios técnicos, viene a identificarse con un poder de autodisposición del propio ámbito personal reservado. De este modo, en una sociedad tecnificada en que los datos personales se hayan en poder de diversos sujetos públicos y privados, que pueden utilizarlos y cruzarlos, el derecho a la intimidad ha ampliado su alcance, para referirse a cualquier dato cuya utilización por terceros puede determinar las posibilidades de

---

padres del niño, y su principal fuente de información sobre su pasado y sus años de formación, por lo que cualquier limitación de acceso constituye una limitación del derecho a la vida personal y familiar.

[658] Se le ha dado Carta de naturaleza autónoma respecto al derecho de la vida privada y familiar, contemplado inmediatamente antes, en el artículo II-7. Se ha seguido en esto la propuesta del Grupo de Trabajo del Artículo 29, en su Dictamen 4/99, de 7 de septiembre. Su texto completo se puede consultar en el siguiente link http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1999/wp26es.pdf

desarrollo del individuo en sociedad, y su contenido, para integrar facultades positivas que garanticen la efectividad del poder de autodisposición del individuo sobre la información que le concierne[659].

El reconocimiento como un derecho autónomo ha venido muy ligado a la idea, característica y origen del nacimiento de las regulaciones sobre protección de datos, según la cual, datos "no íntimos" y en apariencia "inofensivos", cruzados entre sí, con las posibilidades que permite la informática, permiten generar perfiles que condicionen la vida social de las personas[660].

Una consecuencia de esta concepción es que el concepto de dato personal se ha tornado onmicomprensivo. En efecto, hasta el momento, el concepto de dato personal ha venido siendo interpretado de la forma más amplia

---

[659] Restringiéndonos a la doctrina española –que, no obstante, refleja bien el estado de la cuestión en la doctrina comparada–, entre los primeros, MURILLO DE LA CUEVA, se pronuncia por una conceptuación como derecho autónomo fundado en el artículo 18.4 CE, por contraposición con una noción clásica, defensiva y acotada en su objeto del derecho a la intimidad. En Murillo de la Cueva, P. L. (1990). *El derecho a la autodeterminación informativa.* Madrid: Tecnos, pp. 120-121. Tras la aprobación de la LORTAD, en su autocalificada continuación Murillo de la Cueva, P. L. (1993). *Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal).* Madrid: Centro de Estudios Constitucionales, pp. 27-36. Más recientemente, ha defendido la misma postura en "La construcción del derecho a la autodeterminación informativa", Murillo de la Cueva, P. L. (1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos, 104, pp 35-60.* Madrid: CEPC. Niega la subsunción del derecho a la protección de datos en el derecho a la intimidad Fernández Salmerón, M. (2003) *La protección de los datos personales en las Administraciones Públicas*. Madrid: Civitas, p. 60, o Del Castillo Vázquez, I. C. (2007). Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal. *Foro: Revista de ciencias jurídicas y sociales, 6, pp. 231-254*. Entre los segundos, entre otros, Gay Fuentes, C. (1995). *Intimidad y tratamiento de datos en las Administraciones Públicas,* Madrid: Complutense, pp. 29-30, Parejo Alfonso, L. (1996). El derecho fundamental a la intimidad y sus restricciones. En López Ortega, J. J.(Dir.). *Perfiles del derecho constitucional en la vida privada y familiar*. Madrid: Consejo General del Poder Judicial, pp. 41-42.

[660] A esta idea responde la Recomendación del Consejo de Ministros del Consejo de Europa Rec (2010) 13, de 23 de noviembre de 2010, sobre la protección de las personas en relación con el procesamiento automatizado de datos personales para la creación de perfiles: conecta la creación de perfiles con el riesgo de discriminación de todo género, sexual, racial, religiosa, étnica, por las creencias, las discapacidades o la edad– en directa relación la mayoría de ellas con los datos sensibles– y ataques a los derechos fundamentales de las personas, en particular el derecho a la privacidad, pero también incluidos sus derechos sociales y económicos, y a su dignidad.

posible. La normativa comunitaria –y, siguiéndola, las normativas estatales, entre ellas la española– define dato personal como "toda información sobre una persona física identificada o identificable". La jurisprudencia comunitaria sobre protección de datos considera que toda información que incluya el nombre de una persona es un dato personal a los efectos de la aplicación de la protección de datos, y ello incluso cuando el objetivo pretendido por el solicitante de acceso es información sobre un bien o una actividad, y no sobre una persona[661], y, con más razón, cuando se trata de información sobre los ingresos salariales de una persona[662], o sobre la identidad de las personas que ejercen la representación de intereses empresariales ante las Instituciones[663], o el listado de subvenciones con fondos comunitarios, con expresión de las cantidades, los beneficiarios, y las localidades de residencia de éstos[664]. Este concepto amplio lo ha declarado expresamente en línea con la jurisprudencia del TEDH en torno al artículo 8 CEDH. Esta definición omnicomprensiva está en línea con el Derecho comparado y viene a coincidir con la contenida en los Estándares internacionales aprobados en la "Resolución de Madrid"[665].

---

661 Así lo entienden las distintas normas comunitarias y el propio STJCE de 18 de noviembre de 1999, Asunto C-209/97, Comisión contra Consejo, o de 14 de septiembre de 2000, Asunto C-369/98, *Fischer*, en la medida en que dan por supuesto que los datos sobre cultivos, producción, etc., de una determinada explotación son datos personales en la medida en que aparece el nombre de su titular.

662 STJCE de 20 de mayo de 2003, Asuntos acumulados C-465/00, C-138 y 139/01, *Österreichischer Rundfunk*. El TJCE hace una lectura de la Directiva a la luz del artículo 8 CEDH, entendiendo que: "La recogida de datos nominales sobre los ingresos profesionales de un individuo, para comunicárselos a terceros, está comprendida en el ámbito de aplicación del artículo 8 del CEDH", recordando que el Tribunal Europeo de Derechos Humanos declaró, a este respecto, que los términos «vida privada» no debían interpretarse restrictivamente y que «ninguna razón de principio permite excluir las actividades profesionales [...] del concepto de vida privada»

663 Sentencia del Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager contra Comisión, Asunto T-194/04, y Sentencia del Tribunal de Justicia de 29 de junio de 2010, Comisión contra Bavarian Lager, Asunto C-28/08 P.

664 Sentencia del Tribunal de Justica (Gran Sala) de 9 de noviembre de 2010, *Volker und Markus Schecke* y *Hartmut Eifert*, asuntos acumulados C- 92/09 y C-93/09.

665 Agencia Española de Protección de Datos. (2009). Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal «Resolución de Madrid». En el contexto del presente Documento, se

En España, la LOPD acoge la definición de dato personal de la Directiva 95/46/CE[666]. Sin embargo, esta aproximación no es del todo pacífica. El Grupo de Trabajo del artículo 29 parte de la constatación de que el legislador comunitario pretendió adoptar una noción amplia de dato personal, aunque ese concepto no es ilimitado[667]. Lo que más nos interesa es la interpretación

---

entenderá por: "Dato de carácter personal": cualquier información concerniente a una persona física identificada o que pueda ser identificada a través de medios que puedan ser razonablemente utilizados. La Resolución de Madrid disponible en el link https://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_es.pdf

[666] En concreto, la letra a) del artículo 2 indica que «a efectos de la presente Directiva, se entenderá por: a) «datos personales»: toda información sobre una persona física identificada o identificable (el «interesado»); se considerará identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un número de identificación o uno o varios elementos específicos, característicos de su identidad física, fisiológica, psíquica, económica, cultural o social». Por su parte, la letra a) del artículo 3 LOPD afirma que «a los efectos de la presente Ley Orgánica se entenderá por: a) Datos de carácter personal: cualquier información concerniente a personas físicas identificadas o identificables». Nos encontramos ante un artículo dearrollado por el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. (BOE núm. 17, de 19/01/2008. RLOPD), cuyo apartado f) del artículo 5 nos ofrece una definición de dato de carácter personal como «cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables»; a su vez, la letra o) del mismo artículo recoge la definición de persona identificable en los siguientes términos: «toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante cualquier información referida a su identidad física, fisiológica, psíquica, económica, cultural o social. Una persona física no se considerará identificable si dicha identificación requiere plazos o actividades desproporcionados».

[667] El Dictamen 4/2007 sobre el concepto de datos personales, WP 136, de 20 de junio, establece que el objetivo de las disposiciones de la Directiva es proteger los derechos y libertades fundamentales individuales, en especial el derecho a la intimidad, en lo que se refiere al tratamiento de datos personales. Dicha normativa se diseñó para ser aplicada en aquellas situaciones en los que los derechos individuales pueden correr peligro, y por ello necesitados de protección. El ámbito de aplicación de las normas de protección de datos no debe llevarse a su extremo, si bien, debe evitarse una limitación indebida del concepto de datos personales. Las autoridades de protección de datos desempeñan una misión fundamental en la búsqueda de una aplicación equilibrada de las mismas. Existen cuatro «componentes» principales que pueden distinguirse en la definición de «datos personales». Se refiere el Dictamen a la expresión «toda información relativa a una persona física identificada o identificable», y considera que la expresión «toda información» sugiere una interpretación lata del concepto, independientemente de la naturaleza o del contenido de la información y del soporte técnico en el que se presente, lo que significa que tanto las informaciones objetivas como las subjetivas sobre una persona, cualquiera que sea su amplitud, y con independencia del soporte técnico que la contenga, pueden considerarse como «dato personal». El requisito

que debemos dar al término «sobre»[668]. Este componente de la definición es crucial, ya que es muy importante determinar con precisión cuáles son las relaciones, los vínculos que importan, y cómo distinguirlos, y que pueden abarcar informaciones que dicen algo de una persona por su contenido, su finalidad o su resultado, pero no a todas aquellas que llevan simplemente asociado un nombre, pero no se refieren a una persona. Se requiere un análisis que se ha de llevar a cabo en cada caso en concreto.

Sin embargo, el Tribunal de Justicia de la Unión Europea, siguiendo la jurisprudencia TEDH en relación al artículo 8 CEDH, considera que los datos económicos o profesionales, tienen también esa consideración[669].

«identificada o identificable» también es analizado, y en particular, se centra en las condiciones que deben darse para poder considerar a una persona como «identificable», y especialmente en los medios que pueden ser razonablemente utilizados por el responsable del tratamiento o por cualquier otra persona para identificar a dicha persona. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf

668 En la versión inglesa de la Directiva este término es traducido como «*relating to*». Article 2 Definitions. For the purposes of this Directive: (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

669 Véase Piñar Mañas J.L. (2010). Concepto de dato personal. En Troncoso Reigada. A, (Dir.). *Comentario a la Ley orgánica de protección de datos de carácter personal*, Madrid: Civitas-Thomson. Se trata de un debate abierto con implicaciones en relación a la transparencia y acceso a la información oficial. Por el momento, prevalece la consideración de toda información asociada al nombre de una persona como información personal bajo la garantía del derecho a la protección de datos. No obstante, hemos de tener presente la limitación al respecto reflejada en los apartados 2 y 3 del artículo 2 del Reglamento de desarrollo de la LOPD. Artículo 2. Ámbito objetivo de aplicación. 2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales. 3. Asimismo, los datos relativos a empresarios individuales, cuando hagan referencia a ellos en su calidad de comerciantes, industriales o navieros, también se entenderán excluidos del régimen de aplicación de la protección de datos de carácter personal. Tal y como afirma la doctrina, se ha intentado decir mediante un Reglamento lo que hubiera correspondido hacer, en su caso, al legislador. El problema viene dado por la falta de rango normativo del Reglamento.

Respecto al ámbito objetivo, en el Derecho europeo, tanto el CEDH como la Carta Europea de Derechos Fundamentales refieren el derecho a los datos personales obrantes en cualquier soporte[670].

En España el Tribunal Constitucional en su sentencia 292/2000, ha desvinculado el derecho fundamental a la protección de datos del carácter automatizado o no del tratamiento, y, mientras que el artículo 2.1 de la LORTAD[671] se refería «a los datos de carácter personal que figuren en ficheros automatizados de los sectores público y privado y a toda modalidad de uso posterior, incluso no automatizado, de datos de carácter personal registrados en soporte físico susceptible de tratamiento automatizado», el artículo 2.1 de la LOPD, de conformidad con la Directiva 95/46/CE, se refiere «a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado». No hay limitación en cuanto al tipo de información, que no tiene por qué ser información escrita, perfectamente puede ser información visual, genética, biométrica, etc., siempre que responda a los requisitos de clasificación por criterios que permitan la recuperación de información atinente a un sujeto determinado. Por su parte, y siguiendo con la evolución, el artículo 2.1 RGPD refiere su aplicación al «tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero».

Por otro lado, en el apartado 2) del artículo 4 RGPD se considera tratamiento a «cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización,

---

670 El Convenio del Consejo de Europa núm. 108 de 1981 extendió su protección a cualquier tratamiento de datos, público o privado, de carácter automatizado, y previendo, a un tiempo, que su ámbito de aplicación pudiera extenderse a cualquier técnica de procesamiento (también a los procesos no automatizados). La Directiva de 1995 y el Reglamento de 2001 abarcan ya todo tipo de tratamientos.

671 Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (BOE de 31 de octubre de 1992. LORTAD)

estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción».

Se mantiene la aplicación del RGPD a los tratamientos no automatizados. Ahora bien, para que los tratamientos no automatizados la Directiva y la LOPD requieren que los datos obren en un fichero, definido éste como un conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.

Esta condición crea una cierta asimetría entre el ámbito de aplicación del derecho de acceso, referido a toda información o documento, y el de la normativa sobre protección de datos, ya que cuando se trata de documentos en soporte no informático que contienen datos personales pero no están ordenados de tal forma que permita la búsqueda de información atendiendo a criterios personales, y que se facilitan a un tercero en un soporte no informático, no entraría en juego el segundo bloque normativo, debiendo resolverse la cuestión de su legalidad desde la exclusiva óptica de la normativa sobre acceso a la información. Por supuesto, se debe recordar que esta situación es temporal, pues la Directiva 95/46/CE quedará derogada el próximo 25 de mayo de 2018[672].

En cuanto al ámbito subjetivo del derecho a la protección de datos, el titular del derecho es la persona a la cual se refiere la información[673], que puede hacer valer su derecho tanto frente a todos los sujetos públicos -no sólo la Administración- y privados, tanto si los datos han sido generados por ellos como si les han sido transmitidos por el afectado o un tercero.

---

[672] Véase el artículo 94 RGPD.

[673] El apartado 4 del artículo 2 del RLOPD establece una limitación, y tipifica expresamente que este reglamento no será de aplicación a los datos referidos a personas fallecidas. No obstante, las personas vinculadas al fallecido, por razones familiares o análogas, podrán dirigirse a los responsables de los ficheros o tratamientos que contengan datos de éste con la finalidad de notificar el óbito, aportando acreditación suficiente del mismo, y solicitar, cuando hubiere lugar a ello, la cancelación de los datos.

1.4 Aproximación al tratamiento de la transparencia en la Unión Europea. Su evolución desde la incipiente idea de política pública asociada a la realización del mercado

1.4.1 La transparencia en la reutilización de la información del sector público. Especial referencia a la evolución que supone la Directiva 2013/37/UE.

Señala TOMÁS MALLÉN[674] que la dinámica de la construcción europea asentada en las cuatro clásicas libertades[675] económicas ha comportado una concepción de la transparencia guiada por una mínima intervención de las instituciones europeas, tendentes a asegurar la fluidez del tráfico mercantil.

Dicha evolución puede apreciarse en la Directiva 2003/98/CE, de 17 de noviembre, relativa a la reutilización de la información del sector público, al recordar como punto de partida inicial en su Considerando primero[676], la finalidad establecida en los Tratados de creación de un mercado interior y de un sistema que impida el falseamiento de la competencia en éste.

Es a esta perspectiva de libre concurrencia, a la que se asocia la política de garantizar la reutilización de los documentos del sector público, y a tal efecto, establece la Directiva una disposición dedicada a la transparencia y a las tarifas aplicables a esta reutilización[677] Por lo demás, con la misma filosofía

---

[674] Tomás Mallén, B. (2015). Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo Derecho europeo de protección de datos*. Valencia: Tirant lo Blanch, 2015.

[675] La doctrina tradicionalmente las ha denominado «Cuatro Libertades Fundamentales», integradas por la libre circulación de mercancías, trabajadores, servicios y capitales.

[676] Considerando 1 «El Tratado prevé la creación de un mercado interior y de un sistema que impida el falseamiento de la competencia en dicho mercado interior. La armonización de las normas y prácticas de los Estados miembros en relación con la explotación de la información del sector público contribuye a la consecución de estos objetivos».

[677] El artículo 7 de la Directiva 2003/98/CE se dedica a la transparencia en los siguientes términos: «las condiciones aplicables, así como las tarifas normales por reutilización de documentos conservados por organismos del sector público deberán ser fijadas y publicadas de antemano, mediante medios electrónicos cuando resulte posible y oportuno. Previa solicitud, el organismo del sector público indicará la base de cálculo utilizada para las tarifas públicas. El organismo del sector público de que se trate deberá también indicar qué factores se tendrán en cuenta en el cálculo de las

de evitar distorsiones a la libre competencia, la otra vertiente de la transparencia reflejada en la Directiva, tiene que ver con la existencia de contratos o acuerdos exclusivos entre organismos públicos y terceros en este ámbito[678].

Como podemos comprobar, no se incluye una definición de transparencia, sino que aparece vinculada con la garantía de condiciones equitativas, justas, proporcionadas y no discriminatorias[679]. La transparencia se pone en conexión con los operadores económicos y el ejercicio de la libertad de empresa.

En la misma línea, se posiciona la Directiva 2013/37/UE de 26 de junio de 2013 por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público, pues reafirma el objetivo primordial del libre comercio[680] de los documentos existentes en poder de los organismos

---

tarifas para casos atípicos. Los organismos del sector público asegurarán que los solicitantes de reutilización de documentos estén informados de las vías de recurso de que disponen para impugnar las decisiones y las prácticas que les afecten».

[678] Artículo 11 Prohibición de los acuerdos exclusivos «1. La reutilización de documentos estará abierta a todos los agentes potenciales del mercado, incluso en caso de que uno o más de los agentes exploten ya productos con valor añadido basados en estos documentos. Los contratos o acuerdos de otro tipo entre los organismos del sector público que conserven los documentos y los terceros no otorgarán derechos exclusivos. 2. No obstante, cuando sea necesario un derecho exclusivo para la prestación de un servicio de interés público, deberá reconsiderarse periódicamente, y en todo caso cada tres años, la validez del motivo que justificó la concesión del derecho exclusivo. Los acuerdos exclusivos establecidos tras la entrada en vigor de la presente Directiva deberán ser transparentes y ponerse en conocimiento del público». Este artículo establece la prohibición de la existencia de contratos o licencias de carácter exclusivo que restrinjan el acceso por parte de terceros a la documentación objeto de las mismas. De este modo, se establecen dos excepciones: una transitoria en su apartado 3, cuando permitía su permanencia en el caso de existir dicha exclusividad en el momento de transposición de la Directiva, hasta diciembre de 2008; y, otra general, para aquellos supuestos en los cuales el establecimiento de ese derecho exclusivo sea necesario para la prestación de un servicio público, si bien establece su revisión cada tres años.

[679] Esta vinculación queda reflejada en el Considerando 8 al establecer que «se necesita disponer de un marco general para las condiciones de reutilización de los documentos del sector público con el fin de garantizar que dichas condiciones sean equitativas, proporcionadas y no discriminatorias».

[680] En el considerando 4 se destaca que «autorizar la reutilización de los documentos en poder de un organismo del sector público les confiere valor añadido para los reutilizadores, para los usuarios finales y para la sociedad en general y, en muchos casos, para el propio organismo público, ya que el fomento de la transparencia y la responsabilidad y las aportaciones de reutilizadores y usuarios finales

del sector público de los Estados miembros. Sin embargo, el valor añadido que confiere la autorización de la reutilización de los documentos para los reutilizadores, para los usuarios y para la sociedad en general, no pueden suponer una limitación a la tutela de los datos personales, por lo que sigue estableciendo excepciones en aras de la protección de los mismos[681].

Se subraya la relevancia de la transparencia como política pública conectada con el principio de responsabilidad de los poderes públicos[682] y se vislumbra la idea de mayor calidad democrática por referencia a la información recopilada, todo ello a la luz del rápido progreso de las comunicaciones electrónicas.

Es, indudablemente, ese progreso el que justifica la modificación de 2013[683]. Así, en el Considerando 5 de la Directiva 2013/37/UE se destaca que «desde

---

permiten al organismo del sector público de que se trate mejorar la calidad de la información recopilada».

681 En concreto, el considerando 11 de la Directiva reconoce que «la presente Directiva debe incorporarse al Derecho interno y aplicarse de forma que se cumplan plenamente los principios relativos a la protección de los datos personales, de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. En particular, conviene señalar que, con arreglo a dicha Directiva, los Estados miembros deben determinar las condiciones en las que sea legal el tratamiento de datos personales. Además, uno de los principios de dicha Directiva consiste en que los datos personales no deben ser tratados posteriormente a una recogida de un modo que sea incompatible con los objetivos determinados, explícitos y legítimos para los que dichos datos fueron recogidos». Se puede comprobar que el alcance de la preocupación por el tratamiento de los datos personales, y cómo puede afectar éste a la sociedad, está presente en un mayor grado que en el texto de la Directiva 2003/98/CE.

682 En el considerando 10 se reitera la conexión entre transparencia y responsabilidad, en estos términos: «la Directiva 2003/98/CE debe aplicarse a los documentos cuyo suministro sea una actividad que incida en el ámbito de la misión de servicio público de los organismos del sector público implicados, definida con arreglo a la legislación o a otras normas de obligado cumplimiento del Estado miembro. En ausencia de tales normas, la misión de servicio público debe definirse de conformidad con la práctica administrativa común del Estado miembro, siempre y cuando el ámbito de las misiones de servicio público sea transparente y se someta a revisión. La misión de servicio público puede definirse con carácter general o caso por caso para los diferentes organismos del sector público».

683 Tomás Mallén, B. (2015). Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo Derecho europeo de protección de datos*. Valencia: Tirant lo Blanch.

la adopción en 2003 del primer conjunto de normas sobre reutilización de la información del sector público, el volumen de datos, incluidos los públicos, ha aumentado exponencialmente en todo el mundo, al tiempo que se están generando y recopilando nuevos tipos de datos. Paralelamente, estamos asistiendo a una evolución permanente de las tecnologías para el análisis, explotación y tratamiento de datos. Esta rápida evolución tecnológica permite la creación de nuevos servicios y aplicaciones basados en el uso, la agregación o la combinación de datos. Las normas de 2003 están desfasadas con respecto a estos rápidos cambios y, como consecuencia de ello, pueden perderse las oportunidades económicas y sociales que ofrece la reutilización de los datos públicos»[684].

Por otra parte, tanto la Directiva 2013/37/UE como la modificada 2003/98/CE, se remiten de modo genérico al cumplimiento pleno de los principios relativos a la protección de los datos personales de conformidad con la Directiva 95/45/CE. Sin embargo, el enfoque de derechos fundamentales sigue siendo accesorio como posible limitación a la libertad de empresa.

Efectivamente, de un lado, el considerando 11 de la Directiva precisa que con arreglo a la Directiva 95/46/CE, «los Estados miembros deben determinar las condiciones en las que sea legal el tratamiento de datos personales. Además, uno de los principios de dicha Directiva consiste en que los datos personales no deben ser tratados posteriormente a una recogida de un modo que sea incompatible con los objetivos determinados, explícitos y legítimos para los que dichos datos fueron recogidos». Pero, de otro lado, la propia Directiva 2013/37/UE confirma en su Considerando 7 que no se introduce un enfoque positivo o principal de la transparencia en términos de acceso a los documentos, dado que «la Directiva 2003/98/CE no incluye obligación alguna respecto del acceso a los documentos ni obliga a autorizar la reutilización de documentos», por si acaso, el Considerando 8

---

[684] Véase el Considerando 5 de la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público. DOUE núm 175, de 27 de junio de 2013.

corrobora que «las modificaciones llevadas a cabo por la presente Directiva [Directiva 2013/37/UE] no tienen por objeto la definición o modificación de los regímenes de acceso en los Estados miembros, que siguen siendo responsabilidad de los mismos».

Pese a ello, una de las enmiendas operadas por la Directiva 2013/37/UE en la previa Directiva 2003/98/CE afecta a la disposición concreta relativa a la transparencia[685] y, concretamente, viene a incidir directamente en el derecho de acceso a documentos, al habilitar a las autoridades nacionales para que puedan compensar con tarifas, objetivas, transparentes y verificables, los costes generados por facilitar ese acceso. En otros términos, esos costes encaminados a satisfacer a los organismos públicos el ejercicio del acceso para reutilización de la información en su poder presentarán un carácter compensatorio y disuasorio en cierto grado, no susceptible de representar una traba al libre mercado[686].

---

[685] Su nueva redacción es, según la Directiva 2013/37/UE: «Artículo 7 Transparencia 1. En el caso de tarifas normales para la reutilización de documentos que estén en poder de organismos del sector público, las condiciones aplicables, así como el importe real de dichas tarifas, incluida la base de cálculo de dichas tarifas, deberán ser fijadas y publicadas de antemano, mediante medios electrónicos cuando resulte posible y oportuno. 2. Cuando se trate de tarifas para la reutilización distintas de las mencionadas en el apartado 1, el organismo del sector público de que se trate indicará por adelantado qué factores se tendrán en cuenta para el cálculo de dichas tarifas. Cuando se solicite, el organismo del sector público de que se trate también indicará cómo se han calculado dichas tarifas en relación con la solicitud de reutilización concreta. 3. Los requisitos mencionados en el artículo 6, apartado 2, letra b), se fijarán de antemano. Se publicarán por medios electrónicos siempre que sea posible y apropiado. 4. Los organismos del sector público asegurarán que los solicitantes de reutilización de documentos estén informados de las vías de recurso de que disponen para impugnar las decisiones y las prácticas que les afecten.».

[686] Así lo justifica el Considerando 22 de la Directiva 2013/37/UE: «cuando los organismos del sector público apliquen una tarifa por la reutilización de documentos, dicha tarifa debe limitarse en principio a los costes marginales. No obstante, debe tomarse en consideración muy especialmente la necesidad de no entorpecer el funcionamiento normal de los organismos del sector público a los que se exige generar ingresos para cubrir una parte considerable de sus gastos derivados de la realización de sus misiones de servicio público o de los gastos relativos a la recogida, producción, reproducción, y difusión de determinados documentos puestos a disposición para su reutilización. En tales casos, los organismos del sector público deben poder cobrar tarifas superiores a los costes marginales. Dichas tarifas superiores a los costes marginales deben establecerse de acuerdo con criterios objetivos, transparentes y verificables, y los ingresos totales obtenidos por el suministro y por autorizar la reutilización de documentos no deben superar el coste de recogida, producción, reproducción y

1.4.2 Acceso del público a los documentos y protección de datos en el Derecho comunitario. Especial referencia al Reglamento (CE) núm 1049/2001, del Parlamento y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión y al Reglamento (CE) núm 45/2001, del Parlamento y del Consejo, de 18 de diciembre de 2001, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos.

Tanto el acceso del público a los documentos, por un lado, como la intimidad y la protección de datos, por otro, son derechos fundamentales consagrados en una amplia gama de textos legislativos a nivel europeo. Estos derechos están profundamente arraigados en las tradiciones constitucionales de los Estados miembros y gozan de un amplio apoyo público. También son unos elementos esenciales del buen gobierno.

Entre ambos derechos no existe ningún rango jerárquico, y en la mayoría de los casos ninguna tensión. Con todo, hay casos en los que sí puede producirse tensión, dado que el objetivo del Reglamento relativo al acceso del público es favorecer el acceso a todos los documentos, mientras que el Reglamento sobre protección de datos debe garantizar la protección de los datos personales.

La aplicación simultánea de ambos Reglamentos se ha percibido, a veces, como un terreno difícil. El Supervisor Europeo de Protección de Datos (SEPD) publicó un documento en el año 2005 con el fin de demostrar que estos derechos deben considerarse complementarios y no opuestos entre

---

difusión, incrementado por un margen de beneficio razonable de la inversión. El requisito de generar ingresos para cubrir una parte considerable de los gastos de los organismos del sector público derivados de la realización de sus misiones de servicio público o de los gastos relativos a la recogida, producción, reproducción, y difusión de determinados documentos no ha de estar incluido en la legislación y puede derivarse, por ejemplo, de las prácticas administrativas de los Estados miembros. Los Estados miembros deben revisar periódicamente dicho requisito».

sí[687]. El documento tiene por objeto proporcionar orientaciones prácticas para los supuestos en que fuera necesario determinar si un documento que contiene datos personales pudiera ser divulgado a un tercero. En síntesis, el Supervisor Europeo de Protección de Datos viene a defender que ante una solicitud de acceso a documentos que contengan datos personales, la normativa a aplicar es la que regula el derecho de acceso, salvo que sea el propio afectado quien pide la información, en cuyo caso nos encontraríamos ante el llamado derecho de acceso de la normativa sobre protección de datos.

1.4.2.1 Aplicación simultánea de ambos Reglamentos

El Reglamento (CE) núm. 1049/2001 relativo al acceso del público responde al hecho de que en la mayoría de las sociedades democráticas existe un interés general por la divulgación de los documentos de las autoridades públicas. Este Reglamento procura por tanto permitir el grado de acceso más amplio posible a los documentos por parte de los ciudadanos de la UE y de las personas físicas y jurídicas que residan o tengan sede en un Estado miembro.

El derecho de acceso del público está limitado por una serie de excepciones, una de las cuales resulta esencial, ya que se refiere a la intimidad y a la protección de datos. El artículo 4 1) b) del Reglamento 1049/2001 afirma expresamente que:

> *«Las instituciones denegarán el acceso a un documento cuya divulgación suponga un perjuicio para la protección de […] la intimidad y la integridad de la persona, en particular de conformidad con la legislación comunitaria sobre protección de los datos personales».*

---

[687] Se trata del informe del Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. *Background Paper Series, 1*.Recuperado en:. https://edps.europa.eu/sites/edp/files/publication/05-07_bp_accesstodocuments_en.pdf

Las palabras iniciales del artículo 4 1) b) tienen valor absoluto: la divulgación se denegará. En la práctica, el artículo 4 1) b) impone tres condiciones que deben cumplirse para que se aplique la excepción al acceso del público: i) debe estar en juego la intimidad del interesado; ii) el acceso del público debe afectar sustancialmente al interesado; y, iii) el acceso del público no está autorizado por la legislación sobre protección de datos.

1.4.2.1.1 ¿Está en juego la intimidad del interesado?

El derecho a la intimidad, tal como se define en el artículo 8[688] CEDH, va más allá de la protección de la vida privada en sentido estricto, pudiendo incluir asimismo aspectos de la vida profesional, pero aun así no carece de límites.

Para que esté en juego la intimidad del interesado debe existir un interés cualificado de una persona involucrada, es decir el documento tiene que contener detalles sobre una persona que por lo general se consideren "personales" o "privados". El mero hecho de que un documento contenga datos personales de carácter general, como el nombre de una persona, no debería normalmente impedir su divulgación. De esta manera, el Supervisor Europeo de Protección de Datos afirma[689] que la divulgación de datos estaría

---

[688] Aunque se ha indicado con anterioridad, por su interés reproduzco de nuevo el texto íntegro del artículo 8 del Convenio Europeo para la protección de los derechos humanos y de las libertades fundamentales (CEDH). Así, por lo que concierne al Derecho al respeto a la vida privada y familiar, expresamente se reconoce que «1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia. 2. No podrá haber injerencia de la autoridad pública en el ejercicio de este derecho, sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás».

[689] En concreto, el Supervisor Europeo de Protección de Datos reconoce: «Disclosure of data would normally fall within the scope of protection, if: i) sensitive data as mentioned in Article 10 of Regulation 45/2001 are involved, such as for instance data concerning health; ii) the honour and reputation of a person is involved; iii) a person could be placed in a false light; iv) embarrassing facts would be disclosed; information given or received by the individual confidentially would be disclosed». *Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. Background Paper Series, 1*, pp 36-37.

normalmente incluida en el ámbito de protección del Reglamento por estar en juego la intimidad del interesado cuando el documento:

 Contenga datos incluidos en la categoría de datos especiales.
 Se refiera al honor y la reputación de la persona.
 Pudiera dar una imagen falsa de la persona.
 Divulgara hechos embarazosos.
 Divulgara información dada o recibida por la persona con carácter confidencial.

El grado de interés del público por los empleados de una administración pública es distinto del interés que suscitan los empleados del sector privado, y ello por dos razones: la obligación de rendir cuentas y la transparencia.

Por otro lado, el empleado de una administración no asiste a reuniones a título personal, sino que participa en ellas con carácter oficial, en representación de un Estado miembro o una institución u organismo de la UE. Por lo tanto, algunos datos personales más generales, relacionados con la función profesional de un empleado de un organismo público, pueden no estar cubiertos por la protección de la vida privada.

1.4.2.1.2 ¿Se ve afectado sustancialmente el interesado?

Para que la divulgación afecte sustancialmente al interesado debe darse cierto grado de perjuicio objetivo a su intimidad. No debería denegarse al público el acceso a los datos si la divulgación de los mismos solo afectara superficialmente al interesado. En bastantes situaciones, el acceso del público a un documento no afecta a la intimidad del interesado, como por ejemplo cuando dichos datos personales ya han sido divulgados anteriormente.

1.4.2.1.3 La divulgación ¿es conforme con la legislación sobre protección de datos?

Al analizar en qué medida la legislación sobre protección de datos permite la divulgación, desempeñan un papel clave el principio del derecho a la información y el principio de proporcionalidad.

1) El principio del derecho a la información

La divulgación de datos personales debe ser compatible con los fines para los que se recabaron (decididos en el momento de su recogida). Si los fines excluían la divulgación a terceros (explícita o implícitamente), la divulgación sería contraria a la letra b) del artículo 4.1 del Reglamento 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos[690]. En este contexto, habría que tener en cuenta las expectativas razonables del interesado en el momento en que se recaban sus datos.

Además, existen posibilidades muy limitadas para la divulgación de datos personales sensibles que revelen el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas o la afiliación a algún sindicato, así como datos sobre la salud o la vida sexual.

El artículo 5 del Reglamento núm. 45/2001 autoriza la divulgación si ésta es necesaria para el cumplimiento de una misión de interés público, en el legítimo ejercicio de una autoridad oficial o de ser necesario para el cumplimiento de una obligación jurídica[691]. Por un lado, se debe aclarar

---

[690] De este modo, el Reglamento 45/2001 afirma en su artículo 4.1 referente a la calidad de los datos, que «los datos personales deberá ser: […] b) recogidos con fines determinados, explícitos y legítimos, y no ser tratados posteriormente de manera incompatible con dichos fines; no se considerará incompatible el tratamiento posterior de datos con fines históricos, estadísticos o científicos, siempre y cuando el responsable del tratamiento establezca las garantías oportunas, en particular para asegurar que los datos no serán tratados con otros fines y que no se utilizarán en favor de medidas o decisiones que afecten a personas concretas».

[691] Conforme a lo estipulado en el artículo 5 del Reglamento 45/2001 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos, el tratamiento de datos personales solo podrá efectuarse si: « El tratamiento de datos personales sólo podrá efectuarse si: i) es necesario para el cumplimiento de una misión de interés público en virtud de los Tratados constitutivos de las Comunidades Europeas o de otros actos legislativos adoptados sobre la base de los mismos o es inherente al ejercicio legítimo del poder público conferido a la institución o al organismo comunitario o a un tercero a quien se comuniquen los datos; o ii) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento; o iii) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas

que esta disposición facilita el acceso del público en el supuesto de que éste fuera necesario para cumplir lo dispuesto por el Reglamento núm 1049/2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión. Por otro lado, se establece una limitación al acceso del público, al no permitir la divulgación ilícita o desproporcionada de datos personales.

El Supervisor Europeo de Protección de Datos considera que este artículo 5 debe considerarse como la contrapartida del artículo 4 1) b) del Reglamento 1049/2001, dado que el término "necesario" implica la aplicación de un criterio de proporcionalidad[692].

2) El principio de proporcionalidad

El criterio de proporcionalidad consta de dos elementos. En primer lugar, hay que analizar en qué medida se ven afectados los derechos del interesado, tal como los garantiza el Reglamento núm 45/2001. La divulgación no puede en ningún caso tener como consecuencia que una persona se vea privada de sus derechos en materia de protección de datos ni que se restrinja indebidamente su ejercicio de dichos derechos. Las excepciones al acceso del público no deben superar los límites de lo adecuado y necesario para alcanzar la finalidad perseguida[693]. El análisis deberá tener en cuenta:

---

precontractuales adoptadas a petición del interesado; o iv) el interesado ha dado su consentimiento de forma inequívoca; o v) es necesario para proteger los intereses esenciales del interesado.

[692] En palabras del propio Supervisor Europeo de Protección de Datos, «Article 5 should be regarded as the counterpart of Article 4 (1) (b), since the term 'necessary' requires a proportionality test» Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. *Background Paper Series, 1* p.39.

[693] Véase la Sentencia del Tribunal de Justicia de las Comunidades Europeas, Consejo de la Unión c. Hautala, de 6 de diciembre de 2001, asunto C-353/99 P. La Sra. Heidi Hautala, miembro del Parlamento Europeo, solicitó al Consejo que le facilitara un informe sobre la exportación de armamento convencional. El objetivo de dicho informe, elaborado por un grupo de trabajo en el marco de la política exterior y de seguridad común (PESC), es mejorar la aplicación coherente de criterios comunes para las exportaciones de armas. En su Decisión de 4 de noviembre de 1997, el Consejo denegó a la Sra. Hautala el acceso al informe ya que éste contenía informaciones sensibles cuya

a) El tipo de datos personales que son objeto del tratamiento;
b) El carácter voluntario u obligatorio de la recogida inicial de los datos personales;
c) La situación del interesado y las consecuencias que podría acarrearle la divulgación al público;
d) Que la divulgación supone para el interesado un perjuicio menor si el documento se transmite en respuesta a una solicitud que si se publica en Internet.

En segundo lugar, si la divulgación ilimitada de un documento tiene como consecuencia que una persona se vea privada de sus derechos fundamentales en materia de protección de datos o que se restrinja indebidamente su ejercicio de dichos derechos, deben considerarse medidas menos restrictivas. Hay que preguntarse si es posible lograr el mismo resultado mediante otras medidas menos restrictivas, por ejemplo,

---

divulgación menoscabaría las relaciones entre la Unión Europeas y países terceros. Según la Decisión 93/731/CE, relativa al acceso del público a los documentos del Consejo, éste puede denegar el acceso a un documento con el fin de proteger el interés público en el ámbito de las relaciones internacionales. El 19 de julio de 1999, el Tribunal de Primera Instancia anuló la Decisión del Consejo y estimó que éste debía examinar la posibilidad de un acceso parcial a los documentos. El Consejo interpuso un recurso de casación contra dicha sentencia del Tribunal de Primera Instancia. El Tribunal de Justicia de las Comunidades Europeas desestima dicho recurso de casación y confirma, de este modo, la sentencia del Tribunal de Primera Instancia. En primer lugar, el Tribunal de Justicia señala que la Decisión 93/731 no obliga ni prohíbe expresamente al Consejo a examinar si puede concederse un acceso parcial a los documentos. Recuerda que el público debe tener un acceso lo más amplio posible a los documentos que poseen la Comisión y el Consejo y rechaza la alegación del Consejo de que la Decisión controvertida se refiera únicamente al acceso a los "documentos" como tales y no al acceso a los elementos de información contenidos en ellos. Por último, el Tribunal de Justicia considera que el Tribunal de Primera Instancia podía legítimamente estimar que el principio de proporcionalidad obliga al Consejo a considerar el acceso parcial a un documento que contenga elementos de información cuya divulgación ponga en peligro uno de los intereses protegidos por la Decisión 93/731. Asimismo, considera el Tribunal de Justicia que la denegación de acceso parcial constituye una medida desproporcionada para garantizar la protección de los elementos de información amparados por las excepciones de la Decisión. El objetivo de protección que persigue el Consejo al denegar el acceso al informe controvertido podría haberse alcanzado incluso en el caso de que el Consejo se hubiera limitado a censurar los pasajes de dicho informe que pueden menoscabar las relaciones internacionales. En consecuencia, el Tribunal de Justicia confirma la sentencia del Tribunal de Primera Instancia y decide que el Consejo no puede limitar sistemáticamente el derecho del público al acceso a los documentos. En el caso de las excepciones enumeradas por los códigos de conducta del Consejo y de la Comisión debe considerarse la posibilidad de una difusión parcial.

concediendo un acceso parcial a los documentos. Debería estudiarse la posibilidad de conceder un acceso parcial al documento, por ejemplo, transmitiéndolo a un tercero sólo después de haber borrado los datos personales. Podrían suprimirse algunas partes o datos de un documento siempre que ello no suponga una carga administrativa excesiva[694].

2 EL ÁMBITO DE APLICACIÓN DE LA LEY DE TRANSPARENCIA Y SU RELACIÓN CON LA LOPD

El Título I de la LTBG se ocupa de regular la transparencia de la actividad pública. Su objetivo primario consiste esencialmente en definir a quién corresponde cumplir con sus obligaciones y cómo debe hacerlo. Todo ello, debe de ser puesto en relación con la LOPD en la medida en la que un mero contraste de estos aspectos con las definiciones de esta última, permite establecer paralelismos con conceptos como el de responsable, el de encargado del tratamiento o el de cesión de datos personales.

2.1 Principio de publicidad, tratamiento y cesiones de datos personales

Desde el punto de vista del derecho a la protección de datos personales, el principio de publicidad remite al concepto de cesión de datos personales. El objetivo primario de la LTBG solo puede lograrse bien facilitando información al ciudadano solicitante, bien mediante su publicación en el llamado Portal

[694] Tal y como establece el Supervisor Europeo de Protección de Datos, el principio de proporcionalidad consta de dos condiciones: i) derogations to public access should remain within the limits of what is appropriate and necessary for achieving the aim in view; ii) the test whether the same result could not be achieved by other less restrictive measures, for instance by giving partial access to the documents Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. *Background Paper Series, 1,* p.39.

de la Transparencia[695] de la Administración General del Estado y sitios equivalentes en otras administraciones.

Por su parte, la letra i) del artículo 3 LOPD se encarga de la definición de cesión o comunicación de datos personales. Así, se considerará cesión o comunicación de datos «toda revelación de datos realizadas a una persona distinta del interesado». Desde este punto de vista, es necesario destacar la importancia que el instituto de la cesión o comunicación de datos personales posee para la garantía del derecho fundamental a la protección de datos[696]. Precisamente, la posibilidad que preveía el artículo 21.1 LOPD de definir cesiones de datos entre administraciones públicas mediante disposiciones de carácter reglamentario, se encuentra en el origen de la archicitada Sentencia del Tribunal Constitucional 292/2000[697] que determinó su inconstitucionalidad. Así, la excepción de la regla del consentimiento para la cesión en una norma infralegal afectaba claramente al contenido esencial del derecho.

La Sentencia del Tribunal Constitucional 17/2013[698] retoma y refuerza este planteamiento afirmando en su fundamento jurídico cuarto que:

---

[695] El artículo 10 LTBG se encarga de su creación y dotación de contenido, y su artículo 11 se encarga de establecer las prescripciones técnicas, y los principios a los que se debe adecuar.

[696] Véase al respecto Messía de la Cerda Ballesteros, J. A. (2003). *La cesión o comunicación de datos de carácter personal*. Madrid: Thomson-Civitas-APDCM.

[697] Aunque a lo largo de este trabajo nos hemos referido en varias ocasiones a ella, sobre todo a sus Fundamentos Jurídicos 6 y 7, el texto completo de la Sentencia 292/2000, de 30 de noviembre de 2000. Recurso de inconstitucionalidad promovido por el Defensor del Pueblo respecto de los arts. 21.1 y 24.1 y 2 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, se puede consultar en http://www.boe.es/boe/dias/2001/01/04/pdfs/T00104-00118.pdf

[698] Véase la Sentencia 17/2013, de 31 de enero de 2013. Recurso de inconstitucionalidad 1024-2004. Interpuesto por el Parlamento Vasco con respecto a diversos preceptos de la Ley Orgánica 14/2003, de 20 de noviembre, de reforma de la Ley Orgánica 4/2000, de 11 de enero, sobre derechos y libertades de los extranjeros en España y su integración social; de la Ley 7/1985, de 2 de abril, reguladora de las bases del régimen local; de la Ley 30/1992, de 26 de noviembre, de régimen jurídico de las Administraciones públicas y del procedimiento administrativo común y de la Ley 3/1991, de 10 de enero, de competencia desleal. Derecho a la protección de datos; garantías del procedimiento administrativo sancionador y competencias en materia de procedimiento administrativo: interpretación conforme de los preceptos legales relativos a la comunicación interadministrativa de

«En conclusión, tal como establece nuestra doctrina, es claro que la Ley Orgánica de protección de datos no permite la comunicación indiscriminada de datos personales entre Administraciones públicas dado que, además, estos datos están, en principio, afectos a finalidades concretas y predeterminadas que son las que motivaron su recogida y tratamiento. Por tanto, la cesión de datos entre Administraciones públicas sin consentimiento del afectado, cuando se cedan para el ejercicio de competencias distintas o que versen sobre materias distintas de aquellas que motivaron su recogida, únicamente será posible, fuera de los supuestos expresamente previstos por la propia Ley Orgánica de protección de datos, si existe previsión legal expresa para ello [art. 11.2 a) en relación con el 6.1 LOPD] ya que, a tenor de lo dispuesto en el art. 53.1 CE, los límites al derecho a consentir la cesión de los datos a fines distintos para los que fueron recabados están sometidos a reserva de ley. Reserva legal que, como es obvio, habrá de cumplir con los restantes requisitos derivados de nuestra doctrina –esencialmente, basarse en bienes de dimensión constitucional y respetar las exigencias del principio de proporcionalidad– para poder considerar conforme con la Constitución la circunstancia de que la norma legal en cuestión no contemple, por tanto, la necesidad de contar con el consentimiento del afectado para autorizar la cesión de datos. Conforme a nuestra doctrina (STC 292/2000, FJ 16) corresponde al legislador determinar cuándo concurre ese bien o derecho que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse. La finalidad de este derecho fundamental es garantizar a la persona un poder de disposición sobre el uso y destino de sus datos con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado, garantizando a los

---

datos, el acceso a los datos del padrón y los registros de personas y bienes de los extranjeros internados (SSTC 292/2000 y 236/2007). El texto completo se puede consultar en http://hj.tribunalconstitucional.es/HJ/docs/BOE/BOE-A-2013-2167.pdf

individuos un poder de disposición sobre esos datos, mientras que, para los poderes públicos, el derecho fundamental a la protección de los datos personales impone la prohibición de que se conviertan en fuentes de esa información sin las debidas garantías; y también el deber de prevenir los riesgos que puedan derivarse del acceso o divulgación indebidas de dicha información (STC 292/2000, FJ 6 in fine*)»*

El asunto objeto de análisis se refiere a una cesión de datos entre administraciones públicas. Sin embargo, los principios que apunta resultan también relevantes desde el punto de vista de la transparencia.

Desde la Exposición de motivos de la LTBG se declara la intención expresa de ésta en avanzar en «la implantación de una cultura de transparencia que impone la modernización de la Administración, la reducción de cargas burocráticas y el empleo de los medios electrónicos para facilitar la participación, la transparencia y el acceso a la información».

2.2 Responsables de ficheros y sujetos obligados. Accountability y Transparencia

Con carácter previo al análisis concreto de la LGTB es necesario considerar la figura del responsable. La Agencia Española de Protección de Datos, en reiterados informes, así como el artículo 5 RLOPD, han permitido una aproximación precisa al significado del término[699].

[699] Conforme el artículo 5.1.q) RLOPD, «Responsable del fichero o del tratamiento: Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados». El apartado 7 del artículo 4 recoge la definición de responsable del tratamiento o responsable «la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros».

Más relevante resulta la consideración del papel que corresponde jugar al responsable de tratar datos personales cuando se enfrenta a la transparencia. El Tribunal Constitucional en su Sentencia 96/2012[700] sitúa al responsable del fichero/tratamiento prácticamente en una posición de garante. Así, el Fundamento Jurídico 11 afirma expresamente:

> *«De todo lo expuesto se deduce que las resoluciones judiciales impugnadas han vulnerado el art. 18.4 CE. Y ello, porque una diligencia preliminar consistente en requerir a una entidad bancaria la entrega de datos personales de sus clientes, sin el previo consentimiento de éstos, para su posterior entrega a una asociación de consumidores que pretende iniciar un proceso para la defensa de los intereses colectivos de consumidores y usuarios, implica un claro límite en el derecho fundamental a la protección de datos de carácter personal (art. 18.4 CE) y, en consecuencia, no es suficiente la existencia de una genérica habilitación legal (*ex *art. 256.1.6 LEC), sino que dicha medida ha de adoptarse mediante resolución especialmente motivada, exteriorizando los elementos de juicio en los que se basa la resolución, de forma que las razones fácticas y jurídicas queden perfectamente expuestas y, además, debe someterse a un estricto juicio de proporcionalidad, como principio inherente del Estado de Derecho, cuya condición de canon de constitucionalidad tiene especial aplicación cuando se trata de proteger derechos fundamentales frente a limitaciones o constricciones que procedan de normas o resoluciones singulares (STC 85/1992, de 8 de junio, FJ 4). Sin embargo, nada de esto se ha hecho en las resoluciones jurídicas impugnadas. Tal vulneración*

---

[700] Sentencia del Tribunal Constitucional 96/2012, de 7 de mayo de 2012. Recurso de amparo 8640-2010. Promovido por la entidad Banco Bilbao Vizcaya Argentaria, S.A. (BBVA), en relación con las diligencias preliminares de juicio acordadas por un Juzgado de Primera Instancia de Madrid. Vulneración del derecho a la tutela judicial efectiva en relación con el derecho a la protección de datos de carácter personal: resolución judicial que ordena la entrega a una asociación de la relación circunstanciada de quienes hubieran contratado con la entidad bancaria determinados productos financieros. http://hj.tribunalconstitucional.es/HJ/docs/BOE/BOE-A-2012-7506.pdf

material del art. 18.4 CE implica, correlativamente, la lesión del derecho a la tutela judicial efectiva (art. 24.1 CE) de la entidad bancaria demandante de amparo que, cuando se opone al requerimiento de entrega de los ficheros informáticos con los datos personales de aquellos de sus clientes que hubieran suscrito determinados productos financieros, datos sobre los que tiene una obligación jurídica de custodia, no obtiene del órgano judicial una respuesta fundada en una aplicación del ordenamiento jurídico conforme a la Constitución, de acuerdo con las exigencias de motivación y proporcionalidad anteriormente referidas».

Esta Sentencia es importante puesto que en ella subyace el principio de Accountability[701], del que se deriva un especial deber de diligencia del responsable del fichero/tratamiento.

---

[701] Los elementos esenciales de la rendición de cuentas articulan las condiciones que deben existir para que una organización establezca, demuestre y pruebe su rendición de cuentas. Es contra estos elementos que se mide la rendición de cuentas de una organización. Conforme reconoció la Federal Trade Commission, «los elementos esenciales son: i) Compromiso de la organización con la rendición de cuentas y adopción de políticas internas consistentes con criterios externos. Una organización debe demostrar su voluntad y capacidad para ser responsable y responsable de sus prácticas de datos. Una organización debe implementar políticas relacionadas con los criterios externos apropiados (que se encuentran en la ley, los principios generalmente aceptados o las buenas prácticas empresariales) y diseñadas para proporcionar al individuo una protección eficaz de la privacidad, implementar mecanismos para actuar sobre esas políticas y supervisarlos posteriormente. Esas políticas y los planes para ponerlas en práctica deben ser aprobadas al más alto nivel de la organización. El compromiso asegura que la implementación de las políticas no estará subordinada a otras prioridades de la organización. Una estructura organizativa debe demostrar este compromiso asignando al personal apropiado la implementación de las políticas y supervisando esas actividades; ii) Mecanismos para poner en práctica las políticas de privacidad, incluyendo herramientas, capacitación y educación. La organización debe establecer mecanismos de desempeño para implementar las políticas de privacidad establecidas. Los mecanismos pueden incluir herramientas para facilitar la toma de decisiones sobre el uso y protección apropiado de los datos, capacitación sobre cómo utilizar esas herramientas y procesos para asegurar el cumplimiento de los empleados que recogen, procesan y protegen la información. Las herramientas y la capacitación deben ser obligatorias para aquellas personas clave involucradas en la recopilación y despliegue de información personal. Las organizaciones responsables deben crear privacidad en todos los procesos de negocio que recogen, usan o administran información personal; iii) Sistemas para revisiones internas de supervisión y aseguramiento y verificación externa. Utilizando el análisis de la gestión de riesgos, las empresas que recopilan y usan información personal deben monitorear y medir si las políticas que han adoptado y aplicado efectivamente manejan, protegen y aseguran los datos. Las organizaciones responsables

establecen estos sistemas de auditoría de desempeño basados en sus propias culturas empresariales. Los sistemas de rendimiento evalúan las decisiones de una organización sobre los datos a lo largo del ciclo de vida de los datos, desde su recopilación hasta su uso para una aplicación particular, su transmisión a través de las fronteras, su destrucción cuando ya no es útil y deben estar sujetos a alguna forma de supervisión[701]. La organización debería establecer programas para asegurar que los mecanismos se usen apropiadamente mientras los empleados toman decisiones sobre la gestión de la información, la seguridad del sistema y el movimiento de los datos en toda la organización ya los proveedores externos y terceros independientes. La organización también debe participar periódicamente - o ser contratada por - la entidad independiente apropiada para verificar y demostrar que cumple con los requisitos de rendición de cuentas. Cuando proceda, la organización puede recurrir a los servicios de su departamento de auditoría interna para desempeñar esta función, siempre y cuando los auditores informen a una entidad independiente de la organización auditada. Dicha verificación también podría incluir evaluaciones por agentes de cumplimiento de la privacidad o de terceros. Los resultados de tales evaluaciones y cualquier riesgo que pudiera descubrirse pueden ser reportados a la entidad apropiada dentro de la organización que asumiría la responsabilidad de su resolución. La verificación externa debe ser confiable y asequible. Los funcionarios de privacidad pueden trabajar con sus departamentos de auditoría para asegurarse de que las auditorías internas se encuentran entre las herramientas disponibles para supervisar la gestión de datos de la organización. Las organizaciones también pueden comprometer a las empresas a realizar auditorías externas formales; iv) Transparencia y mecanismos de participación individual. Para facilitar la participación individual, los procedimientos de la organización deben ser transparentes. La articulación de los procedimientos de información de la organización y las protecciones en un aviso de privacidad publicado permanece clave para el compromiso individual. La organización responsable desarrolla una estrategia para comunicar de manera prominente a los individuos la información más importante. Las comunicaciones exitosas proporcionan transparencia suficiente para que el individuo entienda las prácticas de datos de una organización como él o ella requiere. La organización responsable puede promover la transparencia a través de avisos de privacidad, iconos, videos y otros mecanismos. Cuando sea apropiado, la información en el aviso de privacidad puede formar la base para el consentimiento o elección del consumidor. Si bien el enfoque de rendición de cuentas anticipa situaciones en las que el consentimiento y la elección pueden no ser posibles, también contempla aquellos casos cuando es factible. En tales casos, debe ponerse a disposición del consumidor y debe constituir la base de las decisiones de la organización sobre el uso de los datos. Los individuos deben tener la capacidad de ver los datos o tipos de datos que la organización recopila, detener la recolección y el uso de esos datos en casos en que puede ser inapropiado y corregirlos cuando sean inexactos. Sin embargo, puede haber algunas circunstancias en las que razones de política pública sólidas limitan esa divulgación; y v) Medios de resolución y cumplimiento externo. La organización debe establecer una política de privacidad que incluya un medio para hacer frente a daño que se puedan ocasionar a las personas debido al fracaso de las políticas y prácticas internas. Cuando se produce un daño debido a un fallo de las prácticas de privacidad de una organización o a un lapso en el cumplimiento de sus políticas internas, las personas deben tener acceso a un mecanismo de recurso. En primer lugar, la organización debe identificar a una persona que sirva de primer punto de contacto para la resolución de conflictos y establecer un proceso mediante el cual se revisen y aborden esas quejas. La organización responsable también puede querer contratar los servicios de un servicio de resolución externo para ayudar a resolver y resolver las quejas de los consumidores. Los agentes de terceros, incluidos los programas de sellos y los servicios de solución de controversias, pueden facilitar la interacción del consumidor con la organización y mejorar su reputación para cumplir con sus políticas

El afectado o titular de los datos personales tiene un poder de disposición que solo es posible si existen ciertos deberes prestacionales por parte del responsable del fichero. Así pues, no basta con operar de modo reactivo frente a posibles vulneraciones, ya que existe un conjunto de obligaciones de naturaleza preventiva ordenadas a tutelar el derecho desde el mismo momento de la recogida de la información y durante todo su ciclo de vida.

Evidentemente, esto sitúa al responsable del fichero ante la necesidad de satisfacer con carácter previo, un conjunto de obligaciones de profundo calado, que además, evoluciona hacia la consolidación de un principio jurídico de origen anglosajón, «la accountability», del que deriva un especial deber de diligencia[702].

Una organización responsable demuestra su compromiso con la rendición de cuentas, implementa políticas de privacidad de datos vinculadas a criterios externos reconocidos y establece mecanismos de desempeño para asegurar una toma de decisiones responsable sobre la administración de los datos de acuerdo con las políticas de la organización. Por tanto, y en la práctica, se trata de disponer de un modelo procedimental que garantice el cumplimiento de la legislación sobre protección de datos de modo que se ofrezca un entorno confiable al administrado que repercuta positivamente en la reputación de la organización.

El considerando 74 del RGPD, señala que:

> *«Debe quedar establecida la responsabilidad del responsable del tratamiento por cualquier tratamiento de datos personales realizado*

---

y cumplir con sus obligaciones con los individuos». Federal Trade Commission *Data Protection Accountability: The Essential Elements. A Document for Discussion*. October 2009. The Centre for Information Policy Leadership. https://www.ftc.gov/sites/default/files/documents/public_comments/privacy-roundtables-comment-project-no.p095416-544506-00059/544506-00059.pdf

[702] Martínez Martínez, R. (2014). De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.) *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Thomson-Reuters Aranzadi. p. 251-252.

por él mismo o por su cuenta. En particular, el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas».

Este deber de responsabilidad ha sido definido de diversos modos, una buena aproximación que permite entender la noción la ofrecen los Comisionados de Privacidad de Canadá[703]:

El RGPD va un poco más allá, y el artículo 24, en sus dos primeros apartados, deja un amplio margen de maniobra a la hora de llevar a cabo el tratamiento por parte del responsable. Eso sí, afirma que deberá aplicar las medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme a las estipulaciones del Reglamento. Estas medidas incluirán las oportunas políticas de protección de datos cuando sean proporcionadas en relación con las actividades de tratamiento. De igual manera el artículo 25 introduce los conceptos Privacidad desde el diseño y Privacidad por defecto, conminando al responsable a llevar a cabo las siguientes medidas[704], incorporando una obligación jurídica de diligencia.

---

[703] En este sentido, «Accountability in relation to privacy is the acceptance of responsibility for personal information protection. An accountable organization must have in place appropriate policies and procedures that promote good practices which, taken as a whole, constitute a privacy management program. The outcome is a demonstrable capacity to comply, at a minimum, with applicable privacy laws. Done properly, it should promote trust and confidence on the part of consumers, and thereby enhance competitive and reputational advantages for organizations». Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia: *Getting Accountability Right with a Privacy Management Program*. https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf

[704] Artículo 25 Protección de datos desde el diseño y por defecto «1.Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas

2.3 Acceso a los datos personales e interés legítimo en el tratamiento

Cuando el artículo 15.5 de la LTBG regula los límites derivados del respeto al derecho fundamental a la protección de datos, abre una puerta al tratamiento de datos derivado de la información al respecto. En efecto, el precepto dispone:

> *«La normativa de protección de datos personales será de aplicación al tratamiento posterior de los obtenidos a través del ejercicio del derecho de acceso».*

Ahora bien, dicha normativa tiene como presupuesto la integración de los datos en ficheros y su tratamiento, es decir que, fuera de esos presupuestos, no cabe invocar a normativa sobre protección de datos para impedir la divulgación general por el solicitante de la información obtenida conforme a la LTBG.

Lo principal en este artículo 15.5 es la referencia al término «tratamiento». Aunque posteriormente incidiremos sobre ello, basta con señalar que la letra c) del artículo 3 LOPD define el tratamiento de datos como aquellas «operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias». Así, bastaría

---

y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados. 2.El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas. 3.Podrá utilizarse un mecanismo de certificación aprobado con arreglo al artículo 42 como elemento que acredite el cumplimiento de las obligaciones establecidas en los apartados 1 y 2 del presente artículo».

con no hacer nada de estas operaciones con la información a la que hemos accedido, para que no se aplique la LOPD.

No puede deducirse de esta previsión normativa una habilitación expresa para tratar datos obtenidos bien mediante el ejercicio individual del derecho de acceso a información pública, bien a través del Portal de Transparencia. Sin embargo, se deja abierta esta posibilidad. No puede descartarse.

Como bien advierte MARTÍNEZ MARTÍNEZ[705], esto nos obliga a considerar en virtud de qué título se accede a la información. En el caso del acceso individual, es importante subrayar que partimos de un modelo, el del artículo 37 de la Ley 30/1992[706] en el que el acceso era causal, y vamos hacia un modelo de objetivación en el que el interés general determina la necesidad de conceder acceso a una determinada información, y la negativa a este acceso es la que debería fundamentarse en cualquiera de los supuestos previstos en los artículos 14 y 15 de la LTBG. Del mismo modo, en el caso del Portal de Transparencia, ni siquiera se requiere de una iniciativa por parte de quien acceda, corresponde a la Administración una labor proactiva de divulgación de información.

Sin embargo, una vez obtenida la información, si desea ser tratada o reutilizada e incorpora datos personales, la cuestión cambia[707]. En este caso, la finalidad en virtud de la cual se accedió podría ser relevante y quien

---

[705] Martínez Martínez, R.: «De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia» en Valero Torrijos, J. y Fernández Salmerón, M. (coord.) *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Aranzadi: Navarra. 2014. p. 256.

[706] La Disposición derogatoria única de la Ley 39/2015 señala en la letra a) de su apartado segundo que la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común queda derogada expresamente a partir de la entrada en vigor de aquella Ley.

[707] Sobre reutilización véase Fernández Salmerón, M. (2006). El régimen jurídico de la reutilización comercial de la información del sector público: sujetos destinatarios y tipos de información. En Galán Galán, A. y Cerrillo i Martínez, A. (coords.): *La reutilización de la información del sector público*. Granada: Comares, pp. 25-50, y Solernou Viñolas, A. (2006). Los datos personales como límite a la reutilización de la información del sector público. En Cerrillo i Martínez, A. y Galán Galán, A. (Coord.): *La reutilización de la informació del sector público*. Granada: Comares, pp. 83-120.

decida realizar el tratamiento deberá estar sujeto a las estipulaciones del principio de calidad de los datos recogidas en el artículo 4 LOPD. Entre ellas, destaco el principio de finalidad que se encuentra definido en el artículo 4.2 LOPD, conforme al cual:

> *«Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos».*

Ahora bien, esta aproximación finalista choca con dos realidades. La primera de ellas reside en el propio esquema de la LTBG. La finalidad para la que se pone a disposición del público la información no es otra que el control democrático de la acción pública. Es al concepto de reutilización[708] al que debemos apuntar para identificar la finalidad que pueda justificar el tratamiento o la creación de ficheros a partir de la información pública lícitamente obtenida. El principio de reutilización orienta la acción en esta materia.

La segunda, deriva del hecho que las tecnologías de la información han evolucionado hasta el punto de eliminar el nexo de causalidad ínsito en el principio de finalidad. En este sentido, en el análisis masivo de datos personales mediante tecnologías de big data, resulta de mayor importancia el propio tratamiento y los resultados que ofrece que el para o porqué se realiza. A ello se une el hecho de que la multiplicación del volumen de información disponible, junto al abaratamiento de los costes de almacenamiento y procesado, han conseguido que por primera vez en la

---

[708] Apartado c) del Artículo 11 «se fomentará que la información sea publicada en formatos que permita su reutilización, de acuerdo con lo previsto en la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público y en su normativa de desarrollo». Además, el artículo 4.6 LTBG declara expresamente que «la reutilización de documentos que contengan datos de carácter personal se regirá por lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal».

historia pueda prescindirse de la muestra meramente estadística para pasar a poder analizar sencillamente todo.

De este modo, hasta que no se ensayen distintos algoritmos de análisis, es probable que no se sepa qué se va a encontrar o sencillamente que los patrones sean simplemente imprevisibles[709]. Las finalidades tenderán a difuminarse o a hacerse muy generales. Incluso en muy probable que la reutilización de información pública con tecnologías de *big data* conduzca a tratamientos de datos personales con carácter posterior.

Llegados a este punto, la reutilización de datos personales obtenidos por medio de información pública conduce inevitablemente al principio de interés legítimo como fuente de legitimación[710] y a la sentencia del Tribunal Supremo 429/2012, de 8 de febrero de 2012, por la que se deroga el artículo 10.2.b) del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal (RLOPD). La sentencia del Tribunal Supremo trae su origen de la cuestión prejudicial resuelta por el Tribunal de Justicia de la Unión Europea en la sentencia Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo

---

709 Véase Mayer-Schönberger, V. Y Cukier, K. (2013). *Big data: la revolución de los datos masivos*, Madrid: Turner.

710 La Directiva 95/46/CE recoge en su artículo 7 las condiciones que se han de cumplir para que se pueda efectuar el tratamiento de datos personales. Así, el apartado f) del mismo, declara que «Los Estados miembros dispondrá que el tratamiento de datos personales sólo pueda efectuarse si: […] f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva». De igual modo, el interés legítimo se encuentra recogido como criterio de validez para el tratamiento de datos personales en el RGPD. En concreto, su artículo 6 relativo a la licitud del tratamiento, declara «1.El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: […] f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

(FECEMD) (C-469/10) c. Administración del Estado, de 24 de noviembre de 2011, y que declaró la eficacia directa del apartado f) del artículo 7 de la Directiva 95/46/CE. El Tribunal Supremo precisa que un «interés legítimo» no es cualquier interés, ya que se requiere un juicio de ponderación que tenga en cuenta los derechos y libertad de los afectados.

> *«38 Dicho artículo 7, letra f), establece dos requisitos acumulativos para que un tratamiento de datos personales sea lícito, a saber, por una parte, que ese tratamiento de datos personales sea necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, y, por otra parte, que no prevalezcan los derechos y libertades fundamentales del interesado. […] 40 No obstante, ha de tenerse en cuenta que el segundo de esos requisitos exige una ponderación de los derechos e intereses en conflicto, que dependerá, en principio, de las circunstancias concretas del caso particular de que se trate y en cuyo marco la persona o institución que efectúe la ponderación deberá tener en cuenta la importancia de los derechos que los artículos 7 y 8 de la Carta de los Derechos Fundamentales de la Unión Europea confieren al interesado».*

Este es el elemento crucial: el interés legítimo, no es cualquier interés. No es una carta blanca para que los responsables puedan tratar datos, La propia Agencia Española de Protección de Datos salió al paso ese mismo día 24 de noviembre, publicando una nota informativa[711] sobre la Sentencia del Tribunal de Justicia de la Unión Europea. De este modo, llega a afirmar expresamente:

> *«Ello no significa, sin embargo, que la mera invocación de un interés legítimo deba considerarse suficiente para legitimar el tratamiento de datos personales sin el consentimiento del afectado. En los*

[711] La nota de prensa de la Agencia Española de Protección de Datos accesible en http://www.agpd.es/portalwebAGPD/revista_prensa/revista_prensa/2011/notas_prensa/common/noviembre/111124_sentencia_TJUE.pdf

fundamentos de la Sentencia, el propio Tribunal precisa la interpretación que debe darse a dicho artículo, subrayando la necesidad de realizar en cada caso concreto una ponderación entre el interés legítimo de quien va a tratar los datos y los derechos fundamentales de los ciudadanos afectados, con el fin de determinar cuál prevalece atendiendo a las circunstancias concurrentes».

Así pues, será necesario acreditar el interés legítimo y cumplir con las restantes obligaciones que impone la LOPD. No obstante, es importante advertir que el mero interés comercial, económico o de cualquier otro tipo, no será interés legítimo si no se encuentra reconocido y protegido por el Ordenamiento Jurídico[712].

[712] Véase, Martínez Martínez, R. (2012). *Interés legítimo y protección de datos personales en la sentencia de 8 de febrero de 2012 del TS*. Recuperado de http://www.elderecho.com/administrativo/Interes-proteccion-personales-Tribunal-Supremo_11_372805001.html

3 TRANSPARENCIA Y PROTECCIÓN DE DATOS PERSONALES. CRITERIOS LEGALES DE CONCILIACIÓN

3.1 El contenido del derecho a la protección de los datos de carácter personal

El derecho fundamental a la protección de los datos de carácter personal deriva del artículo 18.4 de la CE, el cual[713]

> *«contiene un instituto de garantía de los derechos a la intimidad y al honor y del pleno disfrute de los restantes derechos de los ciudadanos, [y] que es, además, en sí mismo, un derecho fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento automatizado de datos, lo que la Constitución llama "la informática"»*

Se trata de un derecho cuyo contenido y alcance fue determinado por la Sentencia 292/2000 del Tribunal Constitucional, de 30 de noviembre, comentada anteriormente en estas páginas, y a las cuales nos remitimos[714].

---

[713] Conforme a lo manifestado por el Tribunal Constitucional en el Fundamento Jurídico 7º de su Sentencia 290/2000, de 30 de noviembre. Recursos de inconstitucionalidad promovidos por el Consejo Ejecutivo de la Generalidad de Cataluña, el Defensor del Pueblo, el Parlamento de Cataluña y por don Federico Trillo- Figueroa Conde, Comisionado por 56 Diputados del Grupo Parlamentario Popular, contra diversos artículos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal. http://hj.tribunalconstitucional.es/HJ/docs/BOE/BOE-T-2001-330.pdf

[714] Véanse al respecto los Fundamentos Jurídicos 6º y 7º de la STC 292/2000, de 30 de noviembre, de los cuales destacamos las manifestaciones relativas a que «el derecho fundamental a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino, con el propósito de impedir su tráfico ilícito y lesivo para la dignidad y derecho del afectado»; y que su objeto de protección «no se reduce solo a los datos íntimos de la persona, sino a cualquier tipo de dato personal, sea o no íntimo, cuyo conocimiento o empleo por tercero pueda afectar a sus derechos, sean o no fundamentales»

Aunque el nuevo RGPD introduce importantes cambios en relación con los derechos de las personas, las obligaciones de los responsables y de los encargados de los tratamientos, la configuración y las competencias de las autoridades de control y el régimen sancionador, en el ámbito que ahora nos ocupa no va a tener un impacto significativo porque, en esencia, mantiene los mismos principios generales reguladores del régimen jurídico de los tratamientos que actualmente figuran en la Directiva 95/46/CE y están acogidos en nuestra LOPD[715].

El artículo 3 de la LOPD define dato personal como «cualquier información concerniente a personas físicas identificadas o identificables». Esta amplia definición de los datos personales no implica que las informaciones de tal naturaleza no se puedan utilizar por terceros, sino que su tratamiento está sometido a una serie de condiciones y garantías legalmente establecidas. Entre ellas, en primer lugar, destaca la necesidad de que todo tratamiento de datos personales, para ser lícito, ha de basarse en el consentimiento del interesado o en una previsión legal que lo autorice[716], incluidas las recogidas

---

[715] De hecho, el RGPD se refiere en el Considerando 154 a su compatibilidad con «el principio de acceso del público a los documentos oficiales» y, en concreto, dedica su artículo 86 a proclamar esa compatibilidad, remitiendo a lo dispuesto en el Derecho de la Unión o en los derechos nacionales, en los siguientes términos: «los datos personales de documentos oficiales en posesión de alguna autoridad pública o u organismo público o una entidad privada para la realización de una misión en interés público podrán ser comunicados por dicha autoridad, organismo o entidad de conformidad con el Derecho de la Unión o de los Estados miembros que se les aplique a fin de conciliar el acceso del público a documentos oficiales con el derecho a la protección de los datos personales en virtud del presente Reglamento».

[716] La directiva 95/46/CE definió en su artículo 7 las condiciones que se deben producir para la licitud del tratamiento. Los Estados miembros dispondrán que el tratamiento solo puede efectuarse si «a) el interesado ha dado su consentimiento de forma inequívoca, o b) es necesario para la ejecución de un contrato en el que el interesado sea parte o para la aplicación de medidas precontractuales adoptadas a petición del interesado, o c) es necesario para el cumplimiento de una obligación jurídica a la que esté sujeto el responsable del tratamiento, o d) es necesario para proteger el interés vital del interesado, o e) es necesario para el cumplimiento de una misión de interés público o inherente al ejercicio del poder público conferido al responsable del tratamiento o a un tercero a quien se comuniquen los datos, o f) es necesario para la satisfacción del interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos, siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requieran protección con arreglo al apartado 1 del artículo 1 de la presente Directiva». Sin embargo, la redacción de la LOPD es diferente puesto que parece preponderar al consentimiento del afectado como parámetro legitimador del

en el propio artículo 6 de la LOPD, algunas de las cuales tienen especial relevancia en el ámbito que nos ocupa.

Además de contar con una base jurídica que los legitime, los tratamientos de datos personales deberán observar una serie de principios establecidos en el artículo 4 LOPD que configuran su régimen general de protección: i) el de lealtad, que prohíbe la recogida por medios fraudulentos, desleales o ilícitos; ii) el de finalidad, que prescribe que los datos solo se podrán tratar para las finalidades determinadas, explícitas y legítimas para las que se

---

tratamiento de datos personales. En su artículo 6.1 afirme expresamente que «el tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa». De igual modo, en el apartado siguiente se establece que «2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado». Se convendrá conmigo que la redacción difiere a la recogida por la normativa europea. Por su parte, el RGPD recoge en su artículo 6 las condiciones que se han de cumplir para la que se produzca la licitud del consentimiento. Así, «el tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones: a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales; c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento; d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física; e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño. Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones». Parece alinearse con la redacción de la Directiva. Fijémonos que el texto indica «al menos una de las siguientes condiciones». En consecuencia, el consentimiento es una más de las condiciones que legitiman la licitud del tratamiento. No se refleja la preponderancia que, en mi opinión, se desprende del texto de la LOPD. De este modo, el consentimiento no es el "báls mo de Fierabrás" que es capaz de curar todas las dolencias que puede padecer el tratamiento de los datos de carácter personal. Máxime si nos paramos a reflexionar en todas las dolencias y limitaciones que en la actualidad adolece el principio del consentimiento. Volveremos a estas conclusiones en profundidad en el siguiente capítulo.

hayan recogido, sin que puedan destinarse a otras finalidades incompatibles; iii) el de proporcionalidad, que determina que solo podrán tratarse los datos que sean adecuados, pertinentes y no excesivos en relación con la finalidad perseguida, y que habrán de ser cancelados cuando hayan dejado de ser necesarios o pertinentes para dicha finalidad; y, iv) el de calidad, que exige que los datos sean exactos, y se mantengan puestos al día. Junto a todo ello, el responsable de los tratamientos deberá informar a los afectados de su existencia y garantizarles los derechos de acceso, rectificación, oposición y cancelación.

Especial relevancia a los efectos que aquí interesan tiene el régimen legal de la cesión o comunicación de datos personales a terceros. De acuerdo con lo previsto en el artículo 11 de la LOPD, «solo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado». Esta regla sólo puede ser exceptuada cuando la cesión esté autorizada en una ley, o cuando resulte aplicable alguna de las excepciones que el propio artículo 11 de la Ley Orgánica prevé: i) cuando los datos hubieran sido recogidos de fuentes accesibles al público; ii) cuando responda a la libre y legítima aceptación de una relación jurídica; iii) cuando tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal, los Jueces, Tribunales, el Tribunal de Cuentas o instituciones autonómicas análogas, en el ejercicio de sus funciones; iv) cuando se produzca entre Administraciones públicas y tenga por objeto el tratamiento con fines históricos, estadísticos y científicos y, v) cuando la cesión de datos de salud sea necesaria para solucionar una urgencia o para realizar estudios epidemiológicos.

3.2 La delimitación de los conflictos entre transparencia y protección de datos

Entre el ingente volumen de información en poder de las Administraciones públicas¯y de los demás sujetos incluidos dentro del ámbito de aplicación de la Ley de Transparencia— se incluyen numerosas informaciones relativas a personas físicas; datos personales de muy diferente naturaleza y con

orígenes diversos, cuya divulgación sin consentimiento puede generar graves lesiones a los derechos fundamentales de los afectados.

Es necesario tener en cuenta, además, que en muchos casos los datos han sido recopilados, y están siendo tratados sin el consentimiento del interesado, en virtud de la habilitación legal que faculta a las Administraciones para ello cuando su finalidad es el ejercicio de las funciones que tienen legalmente atribuidas, por lo que bien puede ser que el afectado ni siquiera tenga conocimiento de que un organismo o una entidad tiene sus datos personales.

En este mismo orden de cosas, debe advertirse que los datos personales en poder de las Administraciones han sido recogidos con finalidades específicas entre las que, por lo general, no se encuentra la de hacerlos públicos, de manera que su divulgación afecta al principio de limitación de la finalidad.

Afirma RODRÍGUEZ ÁLVAREZ que en términos generales, puede decirse que el conflicto entre el derecho de acceso, o el principio de transparencia y el derecho a la protección de datos surge en la medida en que ambos se proyectan a la vez sobre informaciones en manos de los poderes públicos que contienen datos de carácter personal, desplegando sus respectivos efectos en sentido opuesto: mientras que el derecho de acceso confiere una facultad para conocer la información, el derecho a la protección de datos impide o limita su revelación, sometiéndola a la concurrencia de determinados presupuestos y a la observancia de garantías específicas en aras de la salvaguarda de los derechos de los afectados[717].

Por otra parte, ha de tenerse presente que en un buen número de casos el acceso a la información pública no plantea problemas desde el punto de vista del derecho a la protección de datos. No los plantea, en primer lugar, cuando la información se refiere a personas jurídicas, porque no son titulares

---

[717] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, p. 59.

del derecho, dado que sólo ampara a las personas físicas. No existen tampoco limitaciones derivadas del derecho a la protección de datos cuando se trate de informaciones relativas a personas fallecidas, pues estamos ante un derecho que se extingue con la personalidad, aunque en este caso podrían entrar en juego otros derechos. Y, en tercer lugar, no hay colisión cuando la información se puede proporcionar o divulgar previa disociación de los datos de carácter personal, de modo que no sea posible identificar a las personas afectadas. De hecho, esta fórmula, la publicación de la información previa disociación, debería ser la regla aplicable siempre que los datos personales no sean relevantes para satisfacer el interés público que motiva el acceso a la información.

En definitiva, en correspondencia con el ámbito propio del derecho a la protección de datos, el perímetro de los eventuales conflictos entre los derechos que comentamos se circunscribe a los supuestos en los que la información pública contenga datos relativos a personas físicas identificadas o identificables, quedando fuera todas las informaciones que afecten a personas jurídicas, las que se refieran a personas fallecidas, y todas aquellas que hayan sido previamente disociadas de los datos personales.

La pugna entre el derecho que faculta a conocer la información pública y el que la protege en aras de preservar los derechos fundamentales de los ciudadanos habrá de resolverse partiendo del presupuesto básico de que ninguno de ellos tiene carácter absoluto, sino que han de estar sometidos a límites que son necesarios para preservar otros principios, bienes o derechos también reconocidos en la Constitución. En este sentido, cuando se plantee una tensión o conflicto entre el principio de transparencia o el derecho de acceso a la información pública y el derecho a la protección de datos personales, se deberá buscar una solución equilibrada, atendiendo a las circunstancias concurrentes en cada supuesto, a partir de una ponderación razonada entre el interés público en conocer la información y la incidencia que la divulgación de esa información tiene en los derechos de los afectados. Quedan excluidos, en consecuencia, los automatismos y los apriorismos.

Dado que la ponderación necesaria para resolver la colisión de derechos debe hacerse prestando especial atención a las circunstancias concurrentes en cada caso concreto, se trata de una actividad cuya realización corresponde principalmente al órgano que ha de decidir sobre el acceso o la publicación de la información (sin perjuicio de su ulterior revisión en vía de recurso administrativo o judicial). No obstante, el legislador puede asumir una primera fase de esa ponderación y avanzar determinados elementos que acoten el margen de apreciación del órgano decisorio, estableciendo directrices o criterios que orienten su actuación. Esta fue precisamente, como veremos, la opción que tomó el legislador español al elaborar la LTBG[718].

3.3 La articulación de las relaciones entre transparencia y protección de datos en la Ley 19/2013, de 9 de diciembre

Como se ha apuntado, a diferencia de lo sucedido en el pasado en el que las normas de transparencia y las de protección de datos convivían en nuestro ordenamiento sin conexión expresa entre sí, la LTBG, sí establece un nexo directo con la normativa de protección de datos y, en particular, con la LOPD. Tal y como se anuncia en el apartado III de su Preámbulo,

> *«dado que el acceso a la información puede afectar de forma directa a la protección de los datos personales, la Ley aclara la relación entre ambos derechos estableciendo los mecanismos de equilibrio necesarios. Así, por un lado, en la medida en que la información afecte directamente a la organización o actividad pública del órgano prevalecerá el acceso, mientras que, por otro, se protegen –como no puede ser de otra manera– los datos que la normativa califica como especialmente protegidos, para cuyo acceso se requerirá, con carácter general, el consentimiento de su titular».*

---

[718] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, p. 61.

Dentro de la LTBG, el núcleo de la relación entre ambos regímenes jurídicos se configura en el artículo 15, donde se establecen una serie de reglas y criterios que han de presidir la actuación de los órganos administrativos y judiciales cuando resuelvan los casos de colisión, pero también son relevantes otros preceptos como el artículo 5.3 y la Disposición adicional quinta de la Ley. La redacción del artículo 15 experimentó una sustancial modificación en relación con la propuesta inicial del Gobierno, recogida en el entonces artículo 11 del Anteproyecto de ley, como consecuencia del Informe de la Agencia Española de Protección de Datos[719] cuyas recomendaciones fueron asumidas casi al pie de la letra por el Consejo de Ministros en el Proyecto enviado a las Cortes Generales y que acabaría siendo aprobado por el Parlamento sin apenas modificaciones en este apartado.

3.4 Los parámetros de resolución de conflictos previstos en el artículo 15 de la Ley de Transparencia

El legislador español consideró oportuno incorporar a la LTBG determinadas reglas y criterios que han de presidir la resolución de los eventuales conflictos entre la publicidad o el acceso a la información y la protección de los datos personales. Dedica a ello por entero el artículo 15.

Las previsiones de éste, han de ser aplicadas en todas las decisiones sobre transparencia de los poderes públicos, tanto en las relativas a la publicidad activa como en las concernientes al derecho de acceso a la información pública[720]. Ello no significa que el contenido de sus prescripciones tenga el

---

[719] Con anterioridad hemos hecho referencia a los razonamientos que llevaron a la Agencia a elaborar este Informe. Los mismos han sido puestos de manifiesto por el propio Director de aquella época. http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_preceptivos/Administracion_estado/Leyes/common/2012/2013.12.10_2012-0203_APL-Transparencia.pdf

[720] Así resulta del contenido del apartado tercero del artículo 5 LTBG, al indicar que «serán de aplicación, en su caso, los límites al derecho de acceso a la información pública previstos en el artículo 14 y, especialmente, el derivado de la protección de datos de carácter personal, regulado en el artículo 15. A este respecto, cuando la información contuviera datos especialmente protegidos, la publicidad sólo se llevará a cabo previa disociación de los mismos».

mismo alcance en uno y otro supuesto pues, cuando se exige la ponderación de los derechos e intereses en concurrencia, habrá que tomar en consideración el mayor grado de difusión de la información que, como regla, se produce en los casos de publicidad activa, lo cual puede conducir a resultados distintos en relación con una misma información dependiendo de que se solicite el acceso a la misma por particulares o vaya a ser objeto de publicación por la Administración.

El derecho fundamental a la protección de datos es señalado como un límite al derecho de acceso a la información de las administraciones públicas. En multitud de ocasiones se ha esgrimido como una eficaz barrera para la transparencia de nuestras administraciones. El Anteproyecto de ley ordenaba las relaciones entre transparencia y protección de datos a partir de un esquema muy básico[721], que resultaba innecesariamente limitador del acceso a la información en algunos aspectos, pero cuyo principal problema residía en que, al separarse de las categorías y de la sistemática de la normativa de protección de datos, suscitaba incertidumbres hermenéuticas, germen de potenciales divergencias interpretativas y de la consiguiente inseguridad jurídica[722].

Las directrices para la solución de los eventuales conflictos entre ambos derechos, atienden principalmente a la naturaleza de los datos concernidos

---

[721] Su artículo 11, precedente del actual 15, después de establecer en el apartado primero la diferenciación de regímenes que hemos comentado, disponía lo siguiente: «2. Si la información solicitada contuviera datos especialmente protegidos en los términos de la normativa de protección de datos personales, se denegará el acceso salvo que el titular de los datos consienta expresamente y por escrito su divulgación. 3. Con carácter general y, salvo que en el caso concreto prevalezca la protección de datos personales sobre el interés público en la divulgación que lo impidan, se concederá el acceso a la información que contenga datos vinculados con la organización, funcionamiento o actividad pública del órgano. 4. Asimismo, se podrá conceder el acceso a información que contenga datos personales que no tengan la consideración de especialmente protegidos si, previa ponderación suficientemente razonada, el órgano competente para resolver considera que no perjudica ningún derecho constitucionalmente protegido».

[722] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, pp. 62-66.

y al potencial grado de afectación de la esfera privada que su divulgación pública comportaría.

La LTBG tiene en cuenta esta graduación y ordena los supuestos de colisión entre el derecho de acceso a la información y el de protección de datos personales en función de la naturaleza de los datos afectados, estableciendo tres niveles diferenciados, y proporcionando en cada caso las reglas o criterios que han de presidir la actuación de los órganos de decisión.

3.4.1.1 Los datos personales «especialmente protegidos»

En el primer plano se sitúa el conjunto de los datos más sensibles, aquellos cuya divulgación o conocimiento por terceros, afecta con mayor intensidad a los derechos de la esfera personal y que, por esta razón, disfrutan de una protección reforzada en nuestro ordenamiento jurídico.

Son los que la LOPD denomina «datos especialmente protegidos»[723], categoría dentro de la cual, se distinguen dos modalidades. Por un lado,

---

[723] Aparecen reflejados en su artículo 7, con la siguiente redacción: «1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la CE, nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo. 2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado. 3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente. 4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual. 5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras. 6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto. También podrán ser objeto de

recogidos en el apartado segundo del artículo 7 de la norma, están los que revelen la ideología, afiliación sindical, religión o creencias, que solo podrán ser objeto de tratamiento con el consentimiento expreso y por escrito del afectado; y por otro, los que hagan referencia al origen racial, a la salud y a la vida sexual, que podrán ser tratados no solo cuando el afectado lo consienta expresamente, no se exige que sea por escrito, sino también cuando una ley lo disponga por razones de interés general. Conforme al apartado quinto de este artículo, habría que añadir un tercer grupo, integrado por los datos relativos a la comisión de infracciones penales o administrativas, cuya inclusión en ficheros está reservado a las Administraciones públicas competentes.

Este apartado del Anteproyecto fue modificado siguiendo al pie de la letra la propuesta de la Agencia Española de Protección de Datos para armonizarlo al máximo con la LOPD. La redacción inicial establecía un único criterio, según el cual, si la información solicitada contenía datos especialmente protegidos en los términos de la normativa de protección de datos personales, se denegaría el acceso salvo que el titular de los datos consintiera expresamente y por escrito su divulgación.

En su redacción actual, el primer párrafo del artículo 15.1 de la LTBG sigue un esquema similar al del artículo 7 de la LOPD para determinar los supuestos en los que será legítima la publicación o el acceso a informaciones que contengan estas categorías especiales de datos personales. Así, en su apartado primero dispone que

> *«Si la información solicitada contuviera datos especialmente protegidos a los que se refiere el apartado 2 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, el acceso únicamente se podrá autorizar en caso de que se contase con el consentimiento expreso y por escrito del*

---

tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento».

afectado, a menos que dicho afectado hubiese hecho manifiestamente públicos los datos con anterioridad a que se solicitase el acceso».

En consecuencia, el régimen establecido para la publicación o el acceso a informaciones que contengan datos que revelen ideología, afiliación sindical, religión y creencias, es el mismo que el previsto con carácter general para el tratamiento de este tipo de datos: solo podrá acordarse la publicación o concederse el acceso si el afectado, el titular de los datos, presta su consentimiento «expresamente y por escrito». La especial naturaleza de los datos concernidos exige que el derecho de autodeterminación de los individuos sobre su información personal deba ser reconocido en su máxima expresión, de tal suerte que ni siquiera una ley pueda autorizar la publicación o el acceso en contra de la voluntad del afectado.

La LTBG admite, no obstante, una excepción a este estricto régimen de protección para el supuesto de que el propio titular de los datos los hubiese hecho «manifiestamente públicos» con anterioridad al momento de la publicación o de la solicitud del acceso. Con esta cláusula se acoge una salvedad prevista en el apartado e) del artículo 8.2[724] de la Directiva 95/46/CE, que no había sido incorporada explícitamente a nuestro ordenamiento, pero que la Agencia Española de Protección de Datos viene aplicando en aquellos casos en los que se puede descartar con certeza que el tratamiento de los datos de ideología, afiliación sindical, religión o

[724] El artículo 8 relativo al tratamiento de categorías especiales de datos, expresamente declara «1. Los Estados miembros prohibirán el tratamiento de datos personales que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad. 2. Lo dispuesto en el apartado 1 no se aplicará cuando: […] e) el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial».

creencias vaya a causar lesión alguna al afectado porque él mismo los ha hecho manifiestamente públicos con anterioridad de forma voluntaria[725].

En segundo lugar, el segundo párrafo del artículo 15.1 de la LTBG recoge expresamente que

> *«si la información incluyese datos especialmente protegidos a los que se refiere el apartado 3 del artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, o datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, el acceso sólo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley».*

Conforme a ello, cuando los datos que se pretenden publicar o cuyo acceso se solicita hagan referencia al origen racial, a la salud, a la vida sexual, o se trate de datos relativos a la comisión de infracciones penales o administrativas, únicamente si se cuenta con el consentimiento expreso del titular o existe una norma con rango de ley que lo ampare, se podrá proceder a la publicación o conceder el acceso.

A diferencia de lo que sucede con los derechos especialmente protegidos del primer grupo, en este caso, además del consentimiento del afectado, que si bien ha de ser expreso, no se exige que sea por escrito, se admite un segundo presupuesto habilitarte: la autorización por una norma con rango de ley. Por lo demás, el legislador optó por simplificar las previsiones de la Ley Orgánica y asimilar los datos relativos a infracciones penales y administrativas a los referidos al origen racial, salud y vida sexual.

Critica GUICHOT este apartado indicando que lo más cuestionable es el efecto que supone respecto a la inaccesibilidad a la información sobre

---

[725] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, p. 69.

sanciones administrativas, salvo previsión legal expresa o que se trate de sanciones que conlleven amonestación pública. Información por otra parte que no resulta evidente que pertenezca a la intimidad de las personas, y cuyo conocimiento en ocasiones es crucial para controlar la efectiva aplicación por igual de la ley a todas las personas. Más aun, considerando que incluyen, si se sigue la interpretación que se maneja en el campo de la protección de datos, las sanciones disciplinarias, cuyo conocimiento puede ser de suma relevancia pública para juzgar la actuación administrativa.

Lo más significativo del régimen jurídico de los «datos especialmente protegidos» es que se excluye la aplicación de la técnica general de la ponderación del interés público y el grado de afectación de los derechos para resolver los eventuales conflictos. A la hora de decidir sobre si procede o no publicar datos de esta naturaleza, o si se debe o no conceder el acceso a ellos, solo hay que examinar si concurren los requisitos establecidos por el legislador: el consentimiento expreso y por escrito en unos casos (datos de ideología, afiliación sindical, religión y creencias) y el consentimiento expreso o bien una autorización legal en otros (origen racial, salud, vida sexual e infracciones).

La redacción de ambos postulados deberá modificarse con la entrada en vigor del RGPD. En primer lugar, este tipo de datos personales los clasifica o los denomina «categorías especiales»; los mismos aparecen identificados en el artículo 9.1:

> *«Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física».*

Como podemos apreciar a primera vista, el RGPD añade los datos relativos a *datos genéticos* y *datos biométricos* respecto a los recogidos en la misma categoría de datos por parte de la Directiva 95/46/CE[726] .

La regla general es la necesidad de contar con el consentimiento expreso y por escrito del afectado para poder tratar esta tipología de datos. Sin embargo, el artículo 9.2 RGPD establece toda una serie de excepciones a la aplicación de la regla general del apartado anterior. Entre todas excepciones nos llama la atención la referente al «tratamiento de los datos personales que el interesado ha hecho manifiestamente públicos» recogida en el artículo 9.2.e) RGPD[727].

Según el diccionario de la RAE "manifiestamente" significa con claridad y evidencia, descubiertamente. Por tanto, se requiere un comportamiento subjetivo previo del titular de los datos que de modo claro y evidente haya hecho públicos esos datos especialmente protegidos.

No ofrece tantas dudas la regulación relativa a los datos sobre salud, vida sexual y datos relativos a la comisión de infracciones penales o administrativas que no conllevasen la amonestación pública al infractor, ya que el acceso solo se podrá autorizar en caso de que se cuente con el consentimiento expreso del afectado o si aquél estuviera amparado por una norma con rango de Ley. Este planteamiento coincide en esencia con los informes que la Agencia Española de Protección de Datos ha venido emitiendo en esta materia[728].

---

[726] El Artículo 8 de la Directiva 95/46/CE tipifica como categorías especiales de datos los que revelen el origen racial o étnico, las opiniones políticas, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, así como el tratamiento de los datos relativos a la salud o a la sexualidad.

[727] El contenido de esta excepción es muy similar a la tipificada por el artículo 8.2.e) de la Directiva 95/46/CE «el tratamiento se refiera a datos que el interesado haya hecho manifiestamente públicos o sea necesario para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.

[728] En el apartado sobre cesiones del área Informes Jurídicos, dentro del apartado Resoluciones y Documentos, en el que se publican los informes de la Agencia Española de Protección de Datos pueden consultarse, entre otros, informes sobre: i) Cesión IP a equipos de respuesta de incidentes ciberseguridad (2016-0005); ii) Cesión de datos de condena penal a colegio de médicos de país de la Unión Europea (2012-0382); iii) Acceso por Delegaos de Prevención a Datos sobre daños de salud

Desde aquí comparto la crítica efectuada por MARTÍNEZ MARTÍNEZ[729] al indicar que el legislador debería haber sido más preciso ya que en la realidad, los problemas no se plantean de modo tan preciso y la respuesta o solución deberá guiarse por ciertos principios básicos:

La concurrencia de una legitimación previa en origen. La administración de la que se trate solo podrá proporcionar transparencia respecto de aquellos datos que trató legítimamente. Por tanto, por ejemplo, a la hora de decidir sobre si el ciudadano «hizo públicos» ciertos datos, solo debería tener en cuenta aquellos ámbitos que posean relación directa con su ámbito competencial. Publicar datos de esa naturaleza porque el sujeto los hizo públicos en su entorno de red social parece apuntar más a una inadmisible indexación del ciudadano por el Estado.

La presencia de una relación de coherencia y proporcionalidad entre los fines que persiga la transparencia y la información que se publica. Cuando afecte a datos personales el empleo de los criterios que se vienen analizando no puede servir de excusa para «ahorrar trabajo». No se trata de buscar una base jurídica que justifique la publicación de datos personales a toda costa. Como tampoco se trata de lo contrario. Nos referimos a un equilibrio difícil que en muchas ocasiones exigirá un esfuerzo de diligencia en la obtención del consentimiento y/o en todo caso en la preservación de los derechos del afectado en caso de duda.

3.4.1.2 Los datos personales meramente identificativos

En el extremo opuesto a los datos especialmente protegidos, en lo que respecta a su régimen de publicidad y acceso, se sitúan los denominados

---

de trabajadores por accidente de trabajo y enfermedad profesional (2010-0355); iv) Acceso a Historias Clínicas por Agencia Tributaria. Consentimiento del paciente (2010-0242); v) Conservación y/o comunicación y acceso a Historia Clínica del paciente por cese de prestación de servicios sanitarios (2010-0162)

[729] Martínez Martínez, R. (2014). De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.) *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Thomson-Reuters Aranzadi, p. 268.

«datos meramente identificativos relacionados con la organización, el funcionamiento o la actividad pública del órgano», respecto de los cuales el artículo 15.2 de la LTBG dispone que «con carácter general, y salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida, se concederá el acceso a la información» que los contenga.

Este precepto mantiene la redacción inicial que se establecía en el Anteproyecto, salvo la introducción de la precisión «meramente identificativos». El origen de esta modificación se encuentra en la propuesta por parte de la Agencia Española de Protección de Datos al Anteproyecto. Esto resulta sorprendente en la medida en la que el artículo 2.2 del RLOPD[730] excluye de su protección a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en personas jurídicas consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales[731].

---

[730] Artículo 2. Ámbito objetivo de aplicación. «2. Este reglamento no será aplicable a los tratamientos de datos referidos a personas jurídicas, ni a los ficheros que se limiten a incorporar los datos de las personas físicas que presten sus servicios en aquéllas, consistentes únicamente en su nombre y apellidos, las funciones o puestos desempeñados, así como la dirección postal o electrónica, teléfono y número de fax profesionales».

[731] Un ejemplo paradigmático lo encontramos en el Informe 223/2011 de la Agencia Española de Protección de Datos sobre «Publicación en páginas web de Universidad de datos de contacto de sus profesores. Excluido de la LOPD», en el que se indica: «En el supuesto planteado parece claro que la finalidad del fichero de contactos se limita exclusivamente a facilitar el desarrollo y mantenimiento de la actividad docente y formativa ofertada por la Universidad consultante mediante la incorporación de las tecnologías de la información a los métodos de enseñanza, que favorezcan la comunicación profesor-alumno y redunden en la mejora de la actividad académica de la Universidad como institución. Por ello, si los datos identificativos de los profesores universitarios aparecen exclusivamente vinculados a su actividad en el marco de una determinada Administración Pública, y siempre que dicho tratamiento se limite a los datos de los afectados en su mera condición de cargos, administradores o representantes de una empresa o profesores de la Universidad, cabría considerar que estos datos estarían excluidos del marco de aplicación de la Ley 15/1999. En consecuencia, si los datos de contacto a los que se refiere la consulta se enmarcan en el entorno profesional del afectado y su actividad en el marco de su integración profesional en la persona jurídica (Universidad) no será necesario registrar dicho fichero al encontrarse excluido del marco de aplicación de la Ley y por

Sin embargo, el contexto de la transparencia es absolutamente diverso y ajeno a lo que estaba regulado en ese precepto, que tenía como sentido precisamente aclarar que la presencia del nombre de una persona no puede impedir que se conozcan datos relevantes sobre la actuación pública. No solo datos identificativos de funcionarios o autoridades, sino relativos a las decisiones públicas que adoptan que, a su vez, a menudo, implican la mención de nombres de terceras personas, que pueden ser contratistas, beneficiarios de subvenciones, de licencias, etc.

El sentido de este apartado en el Anteproyecto[732] era exponer cómo ese género de información debía ser, por regla general, pública. Es más, la regulación de la publicidad activa en la LTBG muestra claramente este criterio, con la previsión de publicidad en materia de información institucional y organizativa, incluyendo no solo la identificación de los responsables de los diferentes órganos, sino también su perfil y trayectoria personal[733], sino también, se deberá hacer pública[734], como mínimo, la información relativa a

---

consiguiente no se precisaría el consentimiento de los profesores para la comunicación de sus datos de contacto a través de Internet en la página web de la Universidad». El Informe es accesible en http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2011-0223_Publicaci-oo-n-en-p-aa-ginas-web-de-Universidad-de-datos-de-contacto-de-sus-profesores.-Excluido-de-la-LOPD..pdf

732 Artículo 11. Protección de datos personales. «3. Con carácter general y, salvo que en el caso concreto prevalezca la protección de datos personales sobre el interés público en la divulgación que lo impidan, se concederá el acceso a información que contenga datos vinculados con la organización, funcionamiento o actividad pública del órgano».

733 Artículo 6.1 LTBG relativo a la información institucional, organizativa y de planificación, «los sujetos comprendidos en el ámbito de aplicación de este título publicarán información relativa a las funciones que desarrollan, la normativa que les sea de aplicación, así como a su estructura organizativa. A estos efectos, incluirán un organigrama actualizado que identifique a los responsables de los diferentes órganos y su perfil y trayectoria profesional».

734 Véase el apartado 1 del artículo 8 LTBG referente a la información económica, presupuestaria y estadística «Los sujetos incluidos en el ámbito de aplicación de este título deberán hacer pública, como mínimo, la información relativa a los actos de gestión administrativa con repercusión económica o presupuestaria que se indican a continuación: a) Todos los contratos, con indicación del objeto, duración, el importe de licitación y de adjudicación, el procedimiento utilizado para su celebración, los instrumentos a través de los que, en su caso, se ha publicitado, el número de licitadores participantes en el procedimiento y la identidad del adjudicatario, así como las modificaciones del contrato. Igualmente serán objeto de publicación las decisiones de desistimiento

los siguientes actos de gestión administrativa con repercusión económica o presupuestaria: i) todos los contratos; ii) la relación de convenios suscritos; iii) las subvenciones y ayudas públicas concedidas; iv) los presupuestos; v) las cuentas anuales; vi) las retribuciones de los altos cargos; vii) las resoluciones sobre compatibilidad; viii) las declaraciones anuales de bienes y actividades; y, ix) la información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia.

Convenimos con RODRÍGUEZ ÁLVAREZ que viene a establecerse de este modo una suerte de presunción a favor de la publicación o el acceso a este tipo de datos, atendiendo a dos valoraciones objetivas: en primer lugar, el limitado impacto que, por lo general, tiene el conocimiento de los meros

---

y renuncia de los contratos. La publicación de la información relativa a los contratos menores podrá realizarse trimestralmente. Asimismo, se publicarán datos estadísticos sobre el porcentaje en volumen presupuestario de contratos adjudicados a través de cada uno de los procedimientos previstos en la legislación de contratos del sector público. b) La relación de los convenios suscritos, con mención de las partes firmantes, su objeto, plazo de duración, modificaciones realizadas, obligados a la realización de las prestaciones y, en su caso, las obligaciones económicas convenidas. Igualmente, se publicarán las encomiendas de gestión que se firmen, con indicación de su objeto, presupuesto, duración, obligaciones económicas y las subcontrataciones que se realicen con mención de los adjudicatarios, procedimiento seguido para la adjudicación e importe de la misma. c) Las subvenciones y ayudas públicas concedidas con indicación de su importe, objetivo o finalidad y beneficiarios. d) Los presupuestos, con descripción de las principales partidas presupuestarias e información actualizada y comprensible sobre su estado de ejecución y sobre el cumplimiento de los objetivos de estabilidad presupuestaria y sostenibilidad financiera de las Administraciones Públicas. e) Las cuentas anuales que deban rendirse y los informes de auditoría de cuentas y de fiscalización por parte de los órganos de control externo que sobre ellos se emitan. f) Las retribuciones percibidas anualmente por los altos cargos y máximos responsables de las entidades incluidas en el ámbito de la aplicación de este título. Igualmente, se harán públicas las indemnizaciones percibidas, en su caso, con ocasión del abandono del cargo. g) Las resoluciones de autorización o reconocimiento de compatibilidad que afecten a los empleados públicos así como las que autoricen el ejercicio de actividad privada al cese de los altos cargos de la Administración General del Estado o asimilados según la normativa autonómica o local. h) Las declaraciones anuales de bienes y actividades de los representantes locales, en los términos previstos en la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local. Cuando el reglamento no fije los términos en que han de hacerse públicas estas declaraciones se aplicará lo dispuesto en la normativa de conflictos de intereses en el ámbito de la Administración General del Estado. En todo caso, se omitirán los datos relativos a la localización concreta de los bienes inmuebles y se garantizará la privacidad y seguridad de sus titulares. i) La información estadística necesaria para valorar el grado de cumplimiento y calidad de los servicios públicos que sean de su competencia, en los términos que defina cada administración competente».

datos identificativos de una persona cuando se produce el contexto de su actuación en nombre de una Administración u organismo, o en conexión con su funcionamiento o actividad pública; en segundo término, el hecho de que un gran número de documentos administrativos, cuyo conocimiento es de interés público, incorporan datos personales meramente identificativos cuya sola presencia no debería obstaculizar el acceso a la información que contienen. De ahí que sea un criterio generalmente aceptado en los países de nuestro entorno que se deberá facilitar el acceso a los documentos e informaciones relacionadas con la organización, el funcionamiento o las actividades *ad extra* de las Administraciones públicas, aunque con ello se revelen datos identificativos de las personas vinculadas con ellas.

En cuanto a su alcance, la expresión «datos meramente identificativos» ha de ser entendida en sentido estricto, referida solo a los datos básicos de identificación (tales como el nombre y los apellidos, el puesto desempeñado, el teléfono y la dirección de correo profesionales) y siempre que su presencia se dé aislada, nunca en concurrencia con informaciones personales de otra naturaleza.

Sin perjuicio de ello, hay que indicar que el ámbito de aplicación del artículo 15.2 que comentamos no coincide con el del artículo 5.1 de la propia LTBG, por lo que puede permitir la publicación o el conocimiento de más informaciones de las que deben ser objeto de publicidad activa.

En todo caso, se ha de tener presente que la presunción a favor de la publicidad y el acceso establecida en el artículo 15.2 LTBG, no es absoluta. Se concederá, según se dice, «con carácter general». Sin embargo, al mismo tiempo, se dispone que esta regla deberá ser exceptuada en aquellos supuestos en los que concurran circunstancias singulares que determinen que ha de prevalecer «la protección de los datos personales u otros derechos constitucionalmente protegidos» sobre «el interés público en la divulgación». Al configurarse como excepción, deberá ser interpretada en sentido estricto y su aplicación requerirá motivación suficiente.

Por último, destacar que el artículo 15.2 contiene expresamente una excepción que permite modular los efectos del automatismo, en los

siguientes términos «salvo que en el caso concreto prevalezca la protección de datos personales u otros derechos constitucionalmente protegidos sobre el interés público en la divulgación que lo impida». Y es que puede haber supuestos en que la publicidad de determinada información, incluso meramente identificativa, puede implicar para un individuo, o para un colectivo, un grave perjuicio.

3.4.1.3 La ponderación razonada entre en interés público y los derechos de los afectados

Las reglas especiales para la solución de conflictos previstas en la legislación de transparencia, a pesar de su relevancia práctica, tan solo permitirán resolver un reducido porcentaje de los muchos casos en los que la información que se pretende publicar, o a la que se desea acceder, contiene datos personales, pues la mayoría de ellos se situarán en el vasto espacio que media entre los datos «especialmente protegidos» y los «meramente identificativos».

La redacción acogida a propuesta de la Agencia Española de Protección de Datos supone una modificación en la redacción del Anteproyecto[735]. La idea inicial era que el criterio de ponderación era el que regía para aquellos casos del apartado segundo del mismo artículo, en que no se tratase de datos personales relacionados con la organización, funcionamiento o actividad pública del órgano. Para todos estos supuestos intermedios el legislador ha dispuesto en el artículo 15.3 de la Ley que:

> *«Cuando la información solicitada no contuviera datos especialmente protegidos, el órgano al que se dirija la solicitud concederá el acceso previa ponderación suficientemente razonada del interés público en la divulgación de la información y los derechos de los afectados cuyos datos aparezcan en la información solicitada,*

---

[735] Artículo 11. Protección de datos personales «4. Asimismo, se podrá conceder el acceso a información que contenga datos personales que no tengan la consideración de especialmente protegidos si, previa ponderación suficientemente razonada, el órgano competente para resolver considera que no se perjudica ningún derecho constitucionalmente protegido».

en particular su derecho fundamental a la protección de datos de carácter personal».

En consecuencia, cuando los datos afectados no pertenezcan a ninguna de las dos categorías que disponen de un régimen especial, el conflicto habrá de resolverse mediante la técnica de la ponderación, que es el método general de resolución de conflictos entre derechos en nuestro sistema jurídico. Aquella exige sopesar, caso por caso, de un lado, el interés público en conocer la información y, de otro, el impacto que la divulgación de esa información tendría sobre los derechos fundamentales de los afectados, en particular sobre su derecho a la protección de los datos personales, tomando en consideración todas las circunstancias concurrentes, tanto fácticas como jurídicas. La decisión sobre cuál de los derechos o intereses ha de tener prioridad en cada caso concreto deberá adoptarse de manera razonada, con arreglo al principio de proporcionalidad, buscando el punto de equilibrio justo, sin restringir el acceso a la información pública ni los derechos de los afectados más que en la medida que resulte indispensable para conferir la efectividad necesaria a aquel derecho al que se otorga preferencia.

3.4.1.4 Los criterios particulares de ponderación determinados por el legislador

Reconoce RODRÍGUEZ ÁLVAREZ que, como opción de política legislativa, el legislador puede limitarse a establecer la necesidad de realizar una ponderación para resolver los conflictos o, dar un paso más, y proporcionar algunos elementos o criterios que orienten la actuación de los órganos de aplicación, reduciendo así el amplio margen de apreciación que puede resultar de la presencia de conceptos jurídicos indeterminados. Con el fin de introducir un mayor grado de seguridad jurídica y proporcionar a los órganos decisorios determinados elementos orientadores del juicio de ponderación, la Agencia Española de Protección de Datos propuso en su Informe al Anteproyecto de ley, incluir en el texto legislativo una serie de circunstancias objetivas y criterios de valoración que debieran ser tomados en consideración en los procesos de decisión sobre la publicación o sobre el

acceso a informaciones públicas con datos personales. El Gobierno las incorporó al Proyecto de Ley[736].

Como consecuencia de ello, el artículo 15.3 de la LTBG no solo ordena realizar una ponderación, sino que, en su segundo párrafo dispone que:

> *«Para la realización de la citada ponderación, dicho órgano tomará particularmente en consideración los siguientes criterios: a) El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. b) La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos. c) El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos. d) La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad».*

3.4.1.4.1 El menor perjuicio a los afectados derivado del transcurso de los plazos establecidos en el artículo 57 de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español

En relación al primero de los criterios, indicar que resulta la más complicada de aplicar, ya que opera a partir de la aplicación de un lapso temporal definido por el conocimiento o no del paradero de un sujeto[737]. En primer

---

[736] Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria, p. 73.

[737] Al abordar someramente esta cuestión en el Capítulo III, ya se hizo referencia a la crítica de este apartado por parte de la doctrina. Una muestra de ello es Guichot Reina, al respecto, ver superior la nota a pie de página número 503.

lugar, el artículo 57[738] parte de un principio de accesibilidad a documentos en su apartado a) «a no ser que afecten a materias clasificadas de acuerdo con la Ley de Secretos Oficiales o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la Defensa del Estado o la averiguación de los delitos».

En lo que se refiere a los datos personales existen restricciones adicionales fijadas en su apartado c). Este apartado es considerado por MARTÍNEZ MARTÍNEZ como un precepto sencillamente anticuado e ineficaz en el que se encuentra la mayor fuente de riesgo para los derechos fundamentales. En primer lugar, porque en el momento de su redacción el legislador abordaba un supuesto de acceso plano, sin contexto y sin un elemento crucial: *la capacidad de tratamiento*. Por otro lado, gran parte de la información a la que se refiere puede repercutir de modo significativo sobre la intimidad de otras personas[739]. Así pues, urge un cambio que aborde de una vez por todas criterios en realidad más eficientes: la naturaleza de la

---

[738] Artículo cincuenta y siete de la Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. «1. La consulta de los documentos constitutivos del Patrimonio Documental Español a que se refiere el artículo 49.2 se atendrá a las siguientes reglas: a) Con carácter general, tales documentos, concluida su tramitación y depositados y registrados en los Archivos centrales de las correspondientes entidades de Derecho Público, conforme a las normas que se establezcan por vía reglamentaria, serán de libre consulta a no ser que afecten a materias clasificadas de acuerdo con la Ley de Secretos Oficiales o no deban ser públicamente conocidos por disposición expresa de la Ley, o que la difusión de su contenido pueda entrañar riesgos para la seguridad y la defensa del Estado o la averiguación de los delitos. b) No obstante lo dispuesto en el párrafo anterior, cabrá solicitar autorización administrativa para tener acceso a los documentos excluidos de consulta pública. Dicha autorización podrá ser concedida, en los casos de documentos secretos o reservados, por la Autoridad que hizo la respectiva declaración, y en los demás casos por el Jefe del Departamento encargado de su custodia. c) Los documentos que contengan datos personales de carácter policial, procesal, clínico o de cualquier otra índole que puedan afectar a la seguridad de las personas, a su honor, a la intimidad de su vida privada y familiar y a su propia imagen, no podrán ser públicamente consultados sin que medie consentimiento expreso de los afectados o hasta que haya transcurrido un plazo de veinticinco años desde su muerte, si su fecha es conocida o, en otro caso, de cincuenta años, a partir de la fecha de los documentos».

[739] Martínez Martínez, R. (2014). De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.) *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Thomson-Reuters Aranzadi, pp. 262-263.

información, el deber de diligencia del responsable, el deber de diligencia del responsable, el deber de anonimización o la fijación de criterios que permitan resolver el conflicto de derechos. Por otro lado, GUICHOT[740] también se muestra crítico con este apartado por varios motivos. En primer lugar, por cuanto esos plazos se predican en la Ley del Patrimonio Histórico Español de datos que por su naturaleza pueden calificarse de íntimos o especialmente protegidos y a los que, por ello, no puede accederse sin el consentimiento del interesado, y no para el resto de datos personales. Y ahora, en la LTBG, además, se prevén como de aplicación, no a los datos «íntimos» o «especialmente protegidos», sino a los que no lo son. En segundo lugar, por cuanto se trata de un precepto caracterizado por su ambigüedad. Cabe preguntarse ¿a quién corresponde la acreditación de la fecha de fallecimiento de la persona?

3.4.1.4.2 La justificación por los solicitantes de su petición en el ejercicio de un derecho o el hecho de que tengan la condición de investigadores y motiven el acceso en fines históricos, científicos o estadísticos

En relación al primero de los supuestos, el relativo al ejercicio de un derecho, manifestar que se alinea con la problemática manifestada con anterioridad, y conduce directamente a la presencia de un interés legítimo. Sin embargo, el interés aquí comportará necesariamente que el acceso a la información resulte indispensable para la tutela de la esfera de derechos del solicitante ya sea desde el punto de vista del cumplimiento de una obligación, ya lo sea desde el de la invocación o la tutela administrativa o judicial de sus derechos. En cuanto a la delimitación del concepto de fines científicos, históricos o estadísticos, ha sido una constante de la Agencia Española de Protección de Datos remitir a la legislación específica en la materia a fin de delimitar si nos encontramos ante supuestos de esta naturaleza[741]. No resulta tan

---

[740] Véase Guichot Reina, E. (2014). Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, de 9 de diciembre. Madrid: Tecnos, pp 137-138.

[741] Véase el Informe 240/2008 sobre «Acceso a los datos del padrón de los años 1910 y 1911 a efectos de investigación». Disponible en la página web de la Agencia Española de Protección de Datos

sencilla la cuestión cuando el acceso afecte a datos protegidos que deberá regirse por lo expresamente previsto por el del artículo 15.1 de la LTBG. Este último también ha sido duramente criticado al suponer un torpedo en la línea de flotación del derecho de acceso como derecho autónomo vinculado a la ciudadanía y la igualdad de todos en el conocimiento de la información pública. Supone un desconocimiento grave del sentido del derecho como derecho de ciudadanía para la participación y el control democráticos, dando prevalencia en la ponderación a su uso como instrumento al servicio de la tutela de otros derechos individuales o introduciendo diferencias de trato en función de la cualidad del solicitante y de justificación de intereses particulares ajenos a la lógica del derecho y del resto del articulado de la LTBG, que excluye expresamente la necesidad de acreditan interés alguno o de motivar las solicitudes[742]. Además, una vez facilitado el acceso a la información a cualquier solicitante, éste puede hacerla circular libremente a personas en quienes no concurran la condición de investigadores.

3.4.1.4.3 El menor perjuicio de los derechos de los afectados en caso de que los documentos únicamente contuviesen datos de carácter meramente identificativo de aquéllos

El profesor MARTÍNEZ MARTÍNEZ se pregunta ¿Cuál es el menor perjuicio si se ceden nombre y apellidos? Aparentemente ninguno, si bien es cierto es que bastan estos datos para generar un perfil biográfico completo en décimas de segundo mediante un buscador. Seguramente, el menor perjuicio va a consistir en el empleo de técnicas de anonimización ya que la repercusión de un dato meramente identificativo no depende en absoluto de

http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/cesion_datos/common/pdfs/2008-0240_Acceso-a-los-datos-del-padr-oo-n-de-los-a-n-os-1910-y-1911-a-efectos-de-investigaci-oo-n.pdf

[742] Guichot Reina E. (2012). El Proyecto de Ley de Transparencia y acceso a la información pública y el margen de actuación de las Comunidades Autónomas. *Revista Andaluza de Administración Pública, 84*. Sevilla: IAAP, pp 121-122.

esta característica sino más bien del contexto en que se halle y de la finalidad y características del tratamiento.

3.4.1.4.4 La mayor garantía de los derechos de los afectados en caso de que los datos contenidos en el documento puedan afectar a su intimidad o a su seguridad, o se refieran a menores de edad

La concreción de esta «mayor garantía» comporta un juicio de valor de difícil concreción. Solo parece posible aplicar con cierta seguridad los criterios que para el interés legítimo define el artículo 6.1 f) del RGPD.

> *«el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño».*

Mención aparte merece la consideración de los menores de edad. En relación con ellos, el criterio determinante es el de la prevalencia del interés superior del menor[743]. La presencia de este criterio es una constante en todo el Ordenamiento Jurídico. Basta con citar la Sentencia del Tribunal Constitucional 158/2009, que considera el interés superior del menor como límite infranqueable para tales derechos, y cuyas conclusiones deberían trasladarse a nuestro ámbito[744].

---

[743] Grupo de Trabajo del Artículo 29. Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas). WP 160. «El criterio más amplio de legitimación se refiere al interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos (artículo 7, letra f)), siempre que no prevalezca el interés o los derechos y libertades fundamentales del interesado que requiera protección. Para lograr este equilibrio, habrá que considerar especialmente la situación de los niños como personas interesadas en el tratamiento de datos, y servir al objetivo de su interés superior». Dictamen accesible en el siguiente link http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp160_es.pdf

[744] Sentencia del Tribunal Constitucional 158/2009, de 25 de junio. Recurso de amparo promovido por La Opinión de Murcia, S.A., frente a las Sentencias del Tribunal Supremo, de la Audiencia Provincial y de un Juzgado de Primera Instancia de Murcia que le condenaron a abonar una

Por último, no debemos dejar de mencionar el artículo 8 del RGPD en relación a las condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información. Este establece una presunción general al indicar que «el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó». De igual modo, en el apartado 2 se recoge una obligación para el responsable del tratamiento, puesto que deberá hacer los «esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible».

Se ha de observar que no nos encontramos ante una lista tasada. Así, no se excluye el empleo de otros criterios que, a la vista de las circunstancias concurrentes en el caso concreto, resulten relevantes, o incluso prevalentes, para realizar la ponderación y resolver los asuntos en un sentido o en otro. La ley afirma que los criterios se tomarán «particularmente» en

---

indemnización en pleito sobre derecho a la propia imagen. Supuesta vulneración del derecho a la libre información: responsabilidad civil por publicar en un periódico la fotografía de un menor de edad sin consentimiento paterno ni justificación legal. Su Fundamento Jurídico 4 declara expresamente «Ahora bien, cuando se trata, como en el presente caso sucede, de la captación y difusión de fotografías de niños en medios de comunicación social, es preciso tener en cuenta, además de lo anteriormente señalado, que el ordenamiento jurídico establece en estos supuestos una protección especial, en aras a proteger el interés superior del menor, como destacan el Tribunal Supremo en la Sentencia impugnada en amparo (así como las precedentes Sentencias de primera instancia y de apelación que aquélla confirma) y el Ministerio Fiscal en su escrito de alegaciones. En efecto, cabe recordar que, de conformidad con el art. 20.4 CE, las libertades de expresión e información tienen su límite en el respeto a los derechos reconocidos en el título I, en las leyes que lo desarrollan «y, especialmente, en el derecho al honor, a la intimidad, a la propia imagen y a la protección de la juventud y de la infancia». Asimismo, no deben dejar de ser tenidas en cuenta las normas internacionales de protección de la infancia (sobre cuyo valor interpretativo ex art. 10.2 CE no es necesario insistir), y, entre ellas, muy en particular, la Convención de la Naciones Unidas sobre los derechos del niño (ratificada por España por Instrumento de 30 de noviembre de 1990), que garantiza el derecho de los niños a la protección de la ley contra las injerencias arbitrarias o ilegales en su vida privada (art. 16), así como la Resolución del Parlamento Europeo relativa a la Carta europea de los derechos del niño, en la que se establece que «todo niño tiene derecho a no ser objeto por parte de un tercero de intrusiones injustificadas en su vida privada, en la de su familia, ni a sufrir atentados ilegales a su honor» (apartado 29 del § 8 de la Resolución A 3-0172/92 de 8 de julio)».

consideración, de suerte que, si se dan las circunstancias en ellos apreciadas, la decisión deberá orientarse por estos criterios. Esto no impide que, si junto con las circunstancias expresamente contempladas, concurren otras que tengan un mayor peso específico, la balanza se pueda inclinar en sentido opuesto al señalado. Y tampoco implica que, si no se da ninguna de las circunstancias indicadas por el legislador, se tenga que adoptar una decisión contraria al acceso o a la publicación de la información, pues en tales supuestos la ponderación deberá hacerse conforme a criterios generales, tomando en consideración las circunstancias efectivamente concurrentes.

3.4.1.5 La publicación de la información previa disociación de los datos personales

Esta previsión, contenida en el artículo 15.4 LTBG[745], es plenamente coherente con el ámbito material de aplicación de la normativa de protección de datos, pues su presupuesto fundamental es la existencia de información concerniente a «personas físicas identificadas o identificables».

En realidad, una primera aproximación nos podría hacer pensar que este apartado es tautológico, por cuanto en ese caso, la información deja de contener datos personales. Ya hemos visto que el apartado a) del artículo 3 de la LOPD entiende por tales «cualquier información concerniente a personas físicas identificadas o identificables». De igual modo, el artículo 4.1 RGPD establece el concepto de dato personal como « toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos

[745] Expresamente recoge el artículo 15.4 LTBG que «no será aplicable lo establecido en los apartados anteriores si el acceso se efectúa previa disociación de los datos de carácter personal de modo que se impida la identificación de las personas afectadas».

propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Así, si la información originaria ha sido tratada empleando técnicas de anonimización[746], y se han disociado de los datos personales, de suerte que la información resultante no puede ser relacionada con personas identificadas o susceptibles de ser identificadas sin emplear esfuerzos desproporcionados, no debe existir ningún impedimento, desde el punto de vista de la protección de datos, para proceder a su publicación o para conceder el acceso a la información pública.

La LTBG ofrece dos remedios que permitirían evitar de raíz muchos de los problemas enunciados. Por un lado, me refiero a la disociación de los datos de carácter personal, procedimiento establecido en su artículo 15.4, de modo que se impida la identificación de las personas afectadas. En muchas ocasiones, bastará la disociación para conseguir un correcto equilibrio entre transparencia y protección de datos, aunque hay que estar a cada caso ya que, en función de lo singular de la información, en ocasiones las personas a las que van referidas siguen siendo identificables. Sin embargo, hay que diferenciar la anonimización, que es la que nos permitirá aplicar estos preceptos, de la pseudonimización o cualquier otra técnica que permita la llamada reidentificación. Por otro lado, el artículo 16 LTBG, contempla el acceso parcial «previa omisión de la información afectada por el límite salvo que de ello resulte una información distorsionada o que carezca de sentido».

---

[746] Siguiendo las indicaciones del Grupo de Trabajo del Artículo 29, los «datos anónimos» pueden definirse como: «cualquier información relativa a una persona física que no permita su identificación por el responsable del tratamiento de los datos o por cualquier otra persona, teniendo en cuenta el conjunto de medios que puedan razonablemente ser utilizados por el responsable del tratamiento o por cualquier otra persona, para identificar a dicha persona. «Datos anonimizados» serán, por lo tanto, los datos anónimos que con anterioridad se referían a una persona identificable, cuya identificación ya no es posible». En concreto, me refiero a lo estipulado por el Grupo de Trabajo del Artículo 29 en el Dictamen 4/2007 sobre el concepto de datos personales, de 20 de junio. WP 136 y el Dictamen 05/2014 sobre técnicas de anonimización, de 10 de abril. WP 216. Disponibles respectivamente en http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2007/wp136_es.pdf y http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_es.pdf

Uno de los problemas más recientes que nos podemos encontrar es el relativo a la reidentificación de los datos. Asimismo, hay que considerar la posibilidad de conceder el acceso parcial, cuando determinadas partes de la información deba quedar reservada a la vista del juicio de proporcionalidad emitido.

En la práctica, sin embargo, el cumplimiento de las condiciones para excluir la aplicación de la normativa de protección de datos no es una operación tan sencilla como pudiera parecer. La dificultad radica en que, tanto la regulación europea como la Agencia Española de Protección de Datos, establecen como requisito para exonerar su observancia que se trate de una disociación irreversible. Por tanto, solo si se han adoptado las medidas adecuadas para asegurar razonablemente que el proceso de anonimización no puede ser revertido y, en consecuencia, no existen riesgos de reidentificación de las personas concernidas, se podrá considerar que los tratamientos de las informaciones en cuestión no están sometidos a la legislación de protección de datos.

Ahora bien, el cumplimiento de estas condiciones se hace cada día más difícil debido al constante crecimiento del volumen de información disponible y al continuo desarrollo y perfeccionamiento de las tecnologías de interrelación y de análisis de datos[747], procesos que contribuyen a incrementar los riesgos de reidentificación de las personas a partir de informaciones procedentes de diversas fuentes.

Al estar en juego valores, bienes y derechos constitucionales, ha de intentarse su maximización. Por ello, habrá de procederse siempre al otorgamiento del acceso cuando mediante la anonimización de la información solicitada pueda alcanzarse dicha finalidad de conocimiento y control ya que, como establece la normativa sobre protección de datos, la información una vez despersonalizada cae fuera del ámbito de protección

[747] En efecto, y así lo explicaré posteriormente, es posible la utilización de diferentes tratamientos a los datos de carácter personal disociados, los cuales, en la práctica, reviertan esa cualidad. Estoy haciendo referencia a la computación ubicua, lo cual nos traslada a uno de los problemas actuales, pues tiene repercusión directa en el principio del consentimiento.

del derecho. No obstante, la Administración habrá de cerciorarse que la información despersonalizada que facilita no es susceptible de asociación.

Por tanto, estas dos técnicas anunciadas, tanto la anonimización como el acceso parcial, exigirán una enorme diligencia para evitar errores y para impedir que el contexto permita al tercero destinatario de la información inferir datos personales de los sujetos concernidos. De ahí que los órganos decisorios deban emplear una especial diligencia en la selección de las técnicas de anonimización adecuadas en cada caso concreto y poner especial cuidado a la hora de aplicarlas para eliminar o, al menos, minimizar los riesgos de que las informaciones que se consideran disociadas, tras su publicación, acaben siendo vinculadas a personas físicas concretas.

La diligencia y las cautelas han de ser mayores cuando se trata de informaciones que contienen datos especialmente protegidos, en relación con las cuales el artículo 5.3 de la Ley de Transparencia determina que «la publicidad sólo se llevará a cabo previa disociación de los mismos», habida cuenta de la potencial gravedad de las lesiones de derechos fundamentales que pueden derivarse de la divulgación o el conocimiento no consentido de los datos de esta naturaleza. Aparte de este mandato en relación con las informaciones que contengan datos especialmente protegidos, la normativa de transparencia también impone la disociación para la publicación de las resoluciones que apliquen los límites al acceso a la información configurados en el artículo 14 y para la publicación de las resoluciones del Consejo de Transparencia y Buen Gobierno.

Aconseja RODRÍGUEZ ÁLVAREZ que, con independencia de ello, y aunque la Ley no lo establezca de forma expresa, la publicación de la información previa disociación debería ser la regla en todos los casos en los que el conocimiento de los datos personales no sea de interés público, pues de no concurrir este presupuesto no estaría justificada la revelación a terceros de datos personales. Y ello no solo porque cuando están implicados derechos fundamentales siempre han de priorizarse aquellas soluciones que permitan alcanzar la finalidad perseguida con el menor grado de afectación posible de los derechos, sino porque se estaría incumpliendo uno de los principios básicos del régimen de la protección de datos, según el cual, solo se podrán

someter a dicho tratamiento «cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido»[748].

3.5 La colaboración entre la Agencia Española de Protección de Datos y el Consejo de la Transparencia y Buen Gobierno

Como es sabido, el legislador español decidió no asignar la competencia de supervisión y control en materia de transparencia y acceso a la información a la autoridad independiente que ya tenía atribuidas esas mismas funciones en materia de protección de datos, a la Agencia Española de Protección de Datos. Optó por crear una nueva autoridad, el Consejo de Transparencia y Buen Gobierno, al que se encomienda la promoción de la cultura de transparencia y se confieren competencias de control del cumplimiento de las obligaciones de publicidad activa y de garantía del derecho de acceso a la información pública, junto con la de velar por la observancia de las disposiciones de buen gobierno.

Con ello, España se sitúa en línea con los modelos institucionales con dos autoridades de control diferentes, al igual que Francia, Italia, Portugal y Bélgica. Una en el ámbito de la materia de protección de datos y otra en el ámbito de la transparencia. En estos, las relaciones entre ambas han estado tradicionalmente marcadas por cierta tensión y disparidad de criterios.

El principal problema del modelo dual es que, al existir dos órganos independientes con competencias concurrentes sobre un mismo objeto (la delimitación de los ámbitos respectivos de la transparencia y la protección de los datos personales), existe un riesgo real de que se produzcan discrepancias interpretativas e, incluso, de que surjan conflictos entre ellos, con las inevitables consecuencias para la seguridad jurídica que de ello se derivan.

---

[748] Véase el apartado primero del artículo 4 LOPD

Para evitar o, al menos mitigar esos riesgos y sus disfuncionales efectos, la Agencia Española de Protección de Datos propuso la implantación de un mecanismo de coordinación obligatoria que fue acogido en la Disposición adicional quinta[749] de la LTBG sobre colaboración con la Agencia Española de Protección de Datos. En ésta, se prevé que el Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adopten conjuntamente las resoluciones que sean necesarias a fin de determinar los criterios de aplicación de estas reglas, en particular, lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en la LTBG y en la LOPD.

No debemos olvidar, ni obviar, que es la normativa sobre acceso la que rige la publicidad activa o pasiva de información que contiene datos de terceros, y en ese sentido, siendo deseable una interpretación armónica de ambos bloques normativos, dicha interpretación ha sido la efectuada por el legislador en el artículo 15 LTBG, y su interpretación, como la del resto de su articulado, es competencia de las autoridades de transparencia.

---

[749] Disposición adicional quinta. Colaboración con la Agencia Española de Protección de Datos. «El Consejo de Transparencia y Buen Gobierno y la Agencia Española de Protección de Datos adoptarán conjuntamente los criterios de aplicación, en su ámbito de actuación, de las reglas contenidas en el artículo 15 de esta Ley, en particular en lo que respecta a la ponderación del interés público en el acceso a la información y la garantía de los derechos de los interesados cuyos datos se contuviesen en la misma, de conformidad con lo dispuesto en esta Ley y en la Ley Orgánica 15/1999, de 13 de diciembre».

CONCLUSIONES

1. TECNOLOGÍA ACTUAL

Como regla general, para poder proceder al tratamiento de los datos de una persona es necesario que ésta haya manifestado su consentimiento. Este concepto está vinculado a la idea de que el interesado debe poder controlar el uso que se hace de sus datos. El consentimiento es, por tanto, el elemento esencial que, no solo legitima el tratamiento, sino que refleja el poder de disposición del titular sobre sus propios datos.

No obstante, en muchas ocasiones, el consentimiento por parte del interesado se forma sin la necesaria información, y en un entorno de desequilibrio entre las partes, lo que impide considerar que se ha formado de manera libre, requisito esencial del consentimiento válido. De este modo, la falta de información real y el desequilibrio entre las partes pone en riesgo el derecho del titular a decidir sobre sus datos. Expresamente se llega a manifestar por parte del Grupo del Artículo 29 (WP 168) que «la complejidad de las prácticas de recogida de datos, modelos empresariales, relaciones con los vendedores y aplicaciones tecnológicas llega en muchos casos a sobrepasar la capacidad o la voluntad de la persona para tomar decisiones de control sobre el uso e intercambio de información por medio de una elección activa»

Este trabajo plantea, de una parte, que, tal y como lo conocemos en la actualidad, el consentimiento es un mecanismo inadecuado en cuanto expediente legitimador del tratamiento de datos. La concepción individualista que subyace a este enfoque protector no sirve en un mundo donde las prácticas de obtención y análisis masivo de datos son inevitables.

El mayor desafío para la privacidad estriba en que el dato personal es concebido como un derecho fundamental, al tiempo que constituye un activo con valor económico, objeto de explotación comercial. Como mecanismo protector de la privacidad, el consentimiento individual ha fracasado; y desde

luego, sirve de muy poco en el mundo donde las prácticas masivas de captura y análisis de datos banalizan la noción misma de tratamiento consentido. La privacidad basada en los conceptos de control individual de la información, de libre elección y de consentimiento es un mito.

El nuevo marco regulador europeo parece seguir aferrado al mito, y se intenta que recobremos el control de nuestros datos imponiendo condiciones más rigurosas al consentimiento e intensificando los deberes informativos del responsable para «empoderarnos». La reforma sigue centrada, fundamentalmente, en un modelo individualista, como si reforzando la capacidad decisoria de las personas, aumentando sus conocimientos o fomentando que sean «responsables» con sus datos, quedase resuelto el problema de la autodeterminación informativa.

Este planteamiento pasa por alto los límites inherentes al consentimiento informado como medio de control en el actual contexto tecnológico. La intensificación y sofisticación de las técnicas de acumulación y procesamiento de datos personales nos ha privado de opciones reales de saber, y no digamos ya de decidir, qué se hace con nuestra información.

Por un lado, el desarrollo de los equipos informáticos y de las redes de comunicaciones que los conectan ha llevado a un nuevo escenario, en el que la capacidad de cómputo se encuentra repartida entre multitud de dispositivos. Pero no solo evoluciona el soporte tecnológico, sino que también lo hacen los usos de la informática. Así, es un fenómeno creciente la incorporación a los dispositivos que utilizamos cotidianamente, de terminales informáticos conectados a Internet, los cuales muchas veces registran y comunican información relacionada con nuestras actividades.

De esta forma, a la información personal incorporada a los sistemas informáticos, por el fenómeno de la automatización se suma ahora la generada por la monitorización creciente de la vida de las personas. Como resultado de esto, prácticamente todas nuestras actividades e interacciones sociales generan de forma constante un volumen ingente de nueva información personal que queda en manos de terceros.

Por otro, en la actualidad, los ordenadores son capaces de manejar conocimiento, lo que se logra a través de la tecnología denominada inteligencia artificial. Ésta, es empleada con el objetivo de obtener patrones de comportamiento de la población o de grupos. Uno de los resultados es la elaboración de decisiones que pueden afectar a una o más personas.

Conforme las palabras de LESSIG en el año 1998, debemos ser conscientes de que «el mundo en el que estamos entrando está a punto de cambiar estas arquitecturas de privacidad de forma más completa y extensiva que cualquier otro cambio que hayamos presenciado hasta la fecha». La creciente sofisticación de los tratamientos y la proliferación de decisiones automatizadas cada vez dificultan más que una persona pueda conocer lo que verdaderamente se está haciendo con su información, con sus datos personales.

2. INFORMACIÓN AL INTERESADO

La obligación de informar a los interesados cuanto se van a recabar, tratar o almacenar sus datos personales ya estaba recogida en la Directiva 95/46/CE. Sin embargo, el nuevo Reglamento General de Protección de Datos (RGPD) concede una mayor importancia a la información que se debe proporcionar a los ciudadanos cuyos datos van a tratarse, y contempla una lista exhaustiva de los contenidos que deben ser expuestos. Esta obligación debe estar en consonancia con otro importante mandato: el de informar de forma concisa, inteligible y con un lenguaje claro y sencillo.

En la actualidad, abundan los casos de cláusulas informativas o políticas de privacidad cuya lectura puede prolongarse durante horas y que no se caracterizan por su claridad y concisión. La tarea de aunar la obligación de información con la claridad en su exposición, representa todo un reto.

En última instancia, cuando se pretendan ofrecer servicios gratuitos en los que el usuario deba aceptar el tratamiento de su información personal, ha de garantizarse no solo que formalmente ha prestado su consentimiento sino que, además, lo ha hecho específicamente tanto por lo que respecta a la utilización de la aplicación o del producto como, además y de manera

independiente, en cuanto a la cesión de sus datos personales, debiendo ser informado previamente acerca de quién llevará a cabo eventuales tratamientos de su información.

Ahora bien, en la actualidad, la complejidad de las prácticas de recolección de datos, en especial en el ámbito de internet, y los modelos comerciales utilizados, hacen que difícilmente una persona pueda ser consciente y controlar la información que está compartiendo. Resulta imprescindible asegurar no solo la adecuada protección de la privacidad de los sujetos afectados, sino, además y sobre todo, que dispongan de toda la información necesaria de manera transparente a la hora de la toma de decisiones que le afecten.

De ahí que el RGPD tenga como uno de sus objetivos principales reforzar la transparencia y el derecho a la información, de manera que los ciudadanos tengan un conocimiento pleno de quién trata sus datos, de qué manera, con qué fines, durante cuánto tiempo, o de los derechos de que dispone. Con ello se pretende reforzar el control del titular sobre sus datos personales.

Formalmente, los proveedores de servicios y aplicaciones, en el ámbito de internet, cumplen con su deber de informar, pero en la mayoría de las ocasiones, nos encontramos con demasiada información de carácter muy prolijo, abocando a una total falta de transparencia en el deber de información. Asimismo, nos encontramos con unas reglas del juego basadas en cláusulas «lo tomas o lo dejas», «take it or leave it», provocando clara indefensión a los futuros usuarios de estos servicios.

Por otro lado, los usuarios intuyen que la navegación por internet deja rastro. Sin embargo, se ha interiorizado el tratamiento de datos como algo necesario, y un mal menor. Como si se tratara de una conditio sine qua non del acceso a los servicios de la Sociedad de la Información. La población cada vez parece más convencida de que la pérdida de privacidad es inevitable, y casi todos tendemos a aceptarla. El hecho de que haya muchos ciudadanos para los que el bien jurídicamente protegido tiene escaso valor, sobre todo cuando se confronta con otros posibles beneficios, propicia que las iniciativas empresariales más agresivas en materia de protección de

datos encuentren siempre un amplio nicho entre la población que las acepta de forma acrítica, permitiendo de esta forma que se consoliden. Luego, se produce un efecto de adhesión por el que los ciudadanos situados en posiciones intermedias van asumiéndolas paulatinamente. Así, esto acaba provocando la pérdida del control, por parte del sujeto, de sus datos personales, y la consiguiente lesión del derecho. Se cumple de este modo el axioma que indica “si el servicio es gratis, el producto eres tú”.

Asistimos a un paulatino alejamiento entre el ideal de control que se establece en la legislación, y lo que la privacidad supone de veras en la práctica para la mayoría de las personas. Esa divergencia entre promesa legal y plasmación real nos debería hacer reflexionar.

3. EL PRINCIPIO DE TRANSPARENCIA

He comenzado este trabajo haciendo referencia en su INTRODUCCIÓN al concepto de transparencia en el ámbito público, relacionada con la demanda de conocimiento por parte de la sociedad de la información pública y una mayor transparencia administrativa. Todo esto implica tanto un acceso por parte del ciudadano sin necesidad de acreditar un interés legítimo, como una publicación de información a iniciativa de las Administraciones Públicas. Así, se hace referencia, no solo a una solicitud de acceso por parte de ciudadano a información administrativa, sino a la obligación de la Administración de difundir de oficio una determinada información.

Esta demanda de transparencia administrativa estaría vinculada a aquellos movimientos que propugnan una democracia real, una toma del poder por parte de los ciudadanos, y una sociedad más participativa, que tienen como presupuesto el acceso a la información administrativa. Siendo necesaria en muchas ocasiones para que la Administración Pública sirva con objetividad los intereses generales y actúe en cada uno de los procedimientos administrativos con imparcialidad y con sometimiento pleno a la ley y al Derecho. De ese modo, el acceso a la información facilita el respeto de la Administración al principio de legalidad y la vinculación de los poderes públicos a los propios actos.

Ahora bien, esta igualdad en el acceso a la información pública no se proyecta únicamente en las relaciones con la Administración, sino que tiene consecuencias en las relaciones entre particulares. Nos encontramos también ante una demanda de la propia libertad de empresa y del funcionamiento transparente de la economía del mercado, que exige una sociedad abierta. Una manifestación de esto último se produce cuando la solicitud de acceso tiene como finalidad la reutilización con fines comerciales de información en poder de la Administración.

Continuaba la exposición advirtiendo que el acceso a la información pública no es un derecho absoluto, sino que está sometido a límites que deben estar establecidos en una ley, ser legítimos y proporcionales. Entre estos límites, destacamos la protección de datos personales. Por tanto, en ocasiones nos hallamos ante un difícil equilibrio entre los valores constitucionales que demandan una mayor publicidad de la información y aquellos otros que por el contrario exigen reserva. La necesidad de esta reserva se hace manifiestamente notoria cuando la petición de acceso recae sobre datos personales sometidos a tratamiento. Y es que, todos nuestros datos se encuentran en poder de la Administración, y un acceso indiscriminado a estos, puede suponer una transparencia absoluta por parte de los administrados.

Sin embargo, en los últimos años, la información del sector público, no es vista únicamente como un elemento indispensable para el desarrollo de su actividad administrativa. También es considerada como un importante activo cuya reutilización por parte de empresas privadas puede impulsar la actividad económica y la creación de riqueza. La reutilización de información pública está principalmente orientada a fomentar la economía de mercado, valorando los datos que dispone la Administración como un importante activo económico, como materia prima para nuevos productos y servicios digitales.

Ahora bien, este planteamiento quedaría limitado si no apuntáramos brevemente los graves problemas que se plantean con el uso de la reutilización de la información de los poderes públicos, por parte del sector privado. Problemas de muy diversa índole, viéndose afectados tanto la

competencia en el mercado, como el principio de calidad de los datos, pasando por la propiedad intelectual.

Pues bien, el propósito de este trabajo no solo ha sido tratar este ámbito de la transparencia en el ámbito público, y exponer los problemas y soluciones que acarrean, sino el llegar a plantearnos la existencia de una transparencia con un sentido diferente en el ámbito privado. Una transparencia cuya finalidad estriba en cubrir la demanda de información por parte de los particulares para con las empresas. Existe una preocupación cada vez mayor a la hora de obtener todo tipo de información, incluidos los procedimientos internos. Y el Ordenamiento no se queda al margen de ello, y con esta finalidad se crean instrumentos normativos para obligar a las empresas a facilitar esta información. Como derivado de este principio, se amplía el deber de responsabilidad directa o activa por parte de las mismas.

De este modo, el Ordenamiento jurídico relativo a la protección de datos, no permanece al margen, y la transparencia ha quedado reforzada en el RGPD como derecho no solo susceptible de articulación por los particulares ante los poderes públicos, en las relaciones verticales, sino que también se corresponde con las obligaciones positivas que pesan sobre las autoridades públicas a la hora de asegurar la protección de datos bajo el ángulo de la igualdad y equilibrio de posiciones en las relaciones entre individuos, horizontales.

4. DESEQUILIBRIO ENTRE LAS PARTES. CONSENTIMIENTO.

La problemática jurídica se produce porque los conceptos y las categorías jurídicas hasta ahora manejados y que garantizan a los individuos una esfera de privacidad, de desarrollo personal y de control de su información personal, han dejado de ser efectivos.

La propuesta del RGPD de fecha 25 de enero de 2012 detallaba en el artículo 7.4 que: «el consentimiento no constituirá una base jurídica válida para el tratamiento cuando exista un desequilibro claro entre la posición del interesado y el responsable del tratamiento». De igual forma, en los

Considerandos 33 y 34 de la propuesta, se remarcaba que para garantizar el consentimiento libre, éste no puede constituir una base jurídica válida cuando la persona no goza de verdadera libertad de elección; y no está, por tanto, en condiciones de denegar o retirar su consentimiento sin sufrir perjuicio alguno.

Dichas indicaciones no se han trasladado tal cual en la redacción final del RGPD. Ahora bien, el requisito de que el consentimiento se preste de forma libre sigue existiendo. Por ello, en aquellos casos en los que el interesado no tenga una verdadera libertad de elección, su consentimiento estará viciado y no podrá legitimar el tratamiento de datos personales. Si bien es cierto que, esta modificación conlleva una cierta reducción de su virtualidad y, sobre todo, de su aplicación generalizada.

El consentimiento es la llave de todo tratamiento de datos personales. Salvo las excepciones legalmente previstas, el consentimiento da acceso al tratamiento de nuestros datos personales, lo legitima, y permite hablar de un mayor o menor control de los mismos, esto es, de haber sido conscientes o no de que nuestros datos están siendo tratados. El RGPD señala que si el sujeto no tiene total libertad de elección ni posibilidad de revocación, o porque la misma le produzca algún perjuicio, el consentimiento no debería constituir un fundamento jurídico válido para el tratamiento de sus datos. En casos como éstos, la ejecución de un contrato no debería vincularse a la validez del consentimiento si el mismo no es necesario para dicho contrato.

Efectivamente, el consentimiento no constituye un fundamento jurídico válido del artículo 6 del RGPD para el tratamiento de los datos personales, cuando la persona no goza de verdadera libertad de elección y, por tanto, no está en condiciones de denegar o retirar su consentimiento sin sufrir perjuicio alguno. Así, deben establecerse garantías de que el interesado es consciente de haber dado su consentimiento y en qué medida, invirtiéndose la carga de la prueba a favor de la parte más débil.

5. SOLUCIONES REGULATORIAS

Uno de los caminos para lograr ese objetivo se hace pasar por el reajuste de la regla del consentimiento. Para que la decisión individual de aceptar un tratamiento de datos no acarree renunciar al derecho fundamental, se intenta sujetarla a condiciones más rigurosas. Se reproduce el modelo de «consentimiento y control» con el que se busca el «empoderamiento» (empowerment) de los titulares de los datos, es decir, que adquieran o recobren el poder efectivo de decidir qué se hace con su información. A su vez, se quieren redoblar las obligaciones informativas, y quienes procesan datos personales deberán formular las cláusulas de privacidad en términos más sencillos, pero también más completos.

Hasta la fecha, en protección de datos se ha optado por una regulación administrativa, configurando el derecho como un derecho fundamental, relacionado pero distinto del derecho a la intimidad. Y precisamente por ello, las obligaciones que impone la legislación de protección de datos no son intuitivas. El legislador ha querido independizar la protección de datos personales del derecho a la intimidad y dotarle de unas características distintivas propias articuladas en una normativa tan rígida como es la normativa administrativa. Normativa que, hasta la fecha, se ha venido fijando más en las formalidades –leyendas informativas, casillas de consentimiento, declaración de ficheros / tratamientos, existencia de un documento de seguridad o de contratos de encargo de tratamiento– que en una protección sustantiva como son los análisis de impacto en la privacidad, la incorporación efectiva de los principios de privacidad desde el diseño y por defecto y la adopción responsable y comprobable –accountable– de medidas adaptadas a los riesgos detectados.

6. MEDIDAS COMPLEMENTARIAS AL CONSENTIMIENTO INFORMADO POR PARTE DEL INTERESADO

La perspectiva individualista del derecho a la intimidad es claramente insuficiente para hacer frente a los peligros que hoy en día plantea la

explotación incontrolada de la información generada por los ciudadanos. Se debe de acompañar, de medidas de control alternativos o complementarios al consentimiento. Para conseguir reforzar los derechos de los interesados no es suficiente con su reconocimiento en el papel, hacen falta más medidas que les ayuden a ser efectivos. El empoderamiento de los titulares de los datos personales necesita de mejores herramientas que les ayuden a conocer y controlar quién, cómo y para qué se utilizan sus datos personales.

El RGPD pretende dar una vuelta de tuerca a los mismos y crea nuevos principios necesarios para un mayor control de los datos personales. Así, junto al principio de transparencia, se refiere a los principios de privacidad desde el diseño y privacidad por defecto, así como al principio de rendición de cuentas, y toda una batería de medidas obligatorias encaminadas a dotar de un mayor grado de información al usuario relacionada con el tratamiento de sus datos personales. Particularmente, en este momento destaco de ellas la notificación tanto a la Autoridad de Protección de Datos competente, como a los particulares afectados, sobre las posibles brechas de seguridad que se hubieran producido en relación con los tratamientos de datos personales que lleven a cabo. Las propuestas de creación de un certificado y la existencia de iconos normalizados, las desarrollaré en un apartado posterior.

En relación a los principios de privacidad desde el diseño y privacidad por defecto, destacar que este último, es también un mecanismo basado en el consentimiento, ya que consiste en que los sistemas presenten una configuración inicial que no asuma ningún tipo de consentimiento por parte del usuario, el cual debe darlo y manifestarlo expresamente. Por el contrario, el alcance del principio de privacidad desde el diseño, puede ser mucho mayor, en tanto en cuanto, exige que los sistemas se construyan desde el origen cuidando de que sean respetuosos con los derechos de la ciudadanía. Estos principios pretenden generalizar un nuevo paradigma llamado a cambiar las nuevas tecnologías, y nuestra relación con ellas, devolviendo al usuario el control sobre su privacidad, y restaurando su confianza en las empresas privadas e instituciones públicas que tratan sus datos.

Por otro lado, con base en el principio de rendición de cuentas, tanto el responsable como el encargado del tratamiento, deberán garantizar, y están obligado a demostrar, que cada operación de tratamiento de datos que se realice, cumple lo dispuesto en el RGPD. Además, deberán garantizar disponer de los métodos de validación que garanticen la fiabilidad y efectividad de las medidas de seguridad implantadas al respecto. Esta demostración se ha de llevar a cabo de una forma totalmente transparente, aportando el mayor grado de información al interesado.

7. TRANSPARENCIA A LA HORA DE FORMAR EL CONSENTIMIENTO INFORMADO POR PARTE DEL INTERESADO

En el mundo analógico teníamos una frontera razonablemente clara entre la esfera privada y la esfera pública de cada uno de nosotros, y contábamos con ciertas herramientas de control. En el mundo digital sin fronteras y donde la tecnología evoluciona con tanta rapidez, esta frontera y este control parece desdibujarse o, al menos, deben redefinirse con nuevos criterios.

Se ha afirmado que el RGPD reconoce o refuerza nuevos derechos, ocupando un lugar destacado el derecho a la transparencia, que se incorpora al mundo de la protección de datos. La transparencia es un factor clave de cara a un tratamiento equitativo y legítimo de los datos personales. Lo que se busca y se persigue es dotar al usuario del mayor grado de información efectiva posible. De este modo, podrá ser consciente de una manera más clara, y completa, de los tratamientos de datos que se realicen por parte de los responsables o encargados de los mismos.

Ahora bien, ¿cómo se consigue esto? Proponemos salirnos de los cánones actuales, y utilizar a cambio unos planteamientos sencillos. Nada de marear y aplastar al usuario con cientos de cláusulas que en su mayoría son ininteligibles. Se pretende hallar un sistema intuitivo para el usuario.

No supone una novedad presentar la información al usuario por capas. Así lo ha especificado la propia Agencia Española de Protección de Datos, y lo recoge el RGPD. De tal manera que una primera capa de información incluya

un nivel básico de la información requerida, de forma estructurada y muy concentrada, para remitir posteriormente a una segunda capa que contenga esa información más detallada En muchos casos la forma más adecuada será ofreciendo en la primera capa un enlace a otras direcciones web. En otros casos la primera capa podrá dirigir a una segunda que se encuentre impresa en el reverso de un formulario. En todo caso, el objetivo central es que en el primer bloque de información no falte ningún aspecto relevante, aunque sea expuesto de forma sintética, y que para el interesado resulte evidente y sencillo el modo de acceder a la información completa en las siguientes capas. Ejemplos de estos usos los encontramos en la actualidad en los avisos de cámaras de videovigilancia y en los avisos de cookies en páginas web. De hecho, el RGPD prevé que la información pueda ir acompañada de iconos, que la hagan más comprensible, accesible e intuitiva.

En primer lugar, interesa destacar el mecanismo de certificación recogido en el RGPD. Con carácter general, en palabras de la propia AENOR –Asociación Española de Normalización y Certificación–, la certificación puede definirse como «la acción llevada a cabo por una entidad independiente de las partes interesadas mediante la que se manifiesta que una organización, producto, proceso o servicio, cumple con los requisitos definidos en unas normas o especificaciones técnicas».

Se establece en el Considerando 81 RGPD que «la adhesión del encargado a un código de conducta aprobado o a un mecanismo de certificación aprobado puede servir de elemento para demostrar el cumplimiento de las obligaciones por parte del responsable». La certificación, aplicada a la protección de datos personales, además de que pueda servir de elemento para demostrar el cumplimiento, ayuda a generar confianza a los usuarios, y es también relevante por lo que se refiere a conseguir una protección efectiva del interesado en su derecho fundamental a la protección de sus datos personales, pues da lugar a que los responsables o los encargados del tratamiento puedan, previa intervención de un tercero con la pericia, solvencia e independencia necesarias, obtener en su caso un distintivo que acredite que han sido objeto de un proceso de evaluación de conformidad

en materia de protección de datos, debiendo considerarse en cada caso el alcance de la misma.

A diferencia de la Directiva 95/46/CE, en la que no se hacía referencia a la certificación y a otros distintivos como los sellos y marcas de protección de datos, el RGPD sí lo recoge dentro de su articulado. Éste, impone fomentar el establecimiento de mecanismos de certificación, sellos y marcas normalizadas de protección de datos que permitan a los interesados evaluar más rápidamente, de modo fiable y verificable, el nivel de protección de datos de los productos y servicios correspondientes, y ello con el fin de «aumentar la transparencia y el cumplimiento del presente Reglamento». Así se recoge expresamente en el Considerando 100 RGPD, encontrándose regulados los mecanismos de certificación en el artículo 42 del mismo. En él, se prevé la certificación sobre protección de datos para demostrar el cumplimiento de lo dispuesto en el mismo por responsables y encargados del tratamiento. Incluso, se propone la creación de un certificado común: el Sello Europeo de Protección de Datos, a escala europea para crear confianza entre los interesados.

La certificación en protección de datos es un instrumento esencial también para general confianza, tanto para el individuo como para la sociedad. Y al mismo tiempo, es una medida adecuada para que quienes tratan datos personales, ya sean responsables o encargados del tratamiento, consigan contar una ventaja competitiva y generar confianza, además de contar con un elemento para demostrar la adopción de medidas dirigidas al cumplimiento. Por último, indicar conforme el artículo 42.3 RGPD «la adhesión a códigos de conducta aprobados a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento». Los códigos de conducta a los que se refiere este artículo, podrán versar sobre el tratamiento leal y transparente, a la recogida de datos personales, a la información proporcionada al público y a los interesados, etc. Todas ellas referenciadas como una lista ampliable en el artículo 40.2 RGPD, al cual nos remitimos.

Precisamente, aumentar la transparencia y demostrar cumplimiento ante todas las partes interesadas son, y deben ser considerados como tales, los incentivos y beneficios de la certificación en protección de datos, sin perjuicio de que pudiera haber otros.

Como decimos, la certificación apunta a fomentar la transparencia y la autorregulación en el seno de las empresas. Esta forma de proceder les permite identificar y limitar los riesgos ligados al tratamiento de datos personales. Permite igualmente contribuir al cumplimiento de las obligaciones por parte de las empresas delegando una parte de la carga de control a los organismos emisores de los sellos. En España, nuestra LOPD no hace mención alguna en relación a la certificación apuntada. No así la norma homóloga francesa, la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, en su artículo 11.

Es más, en su Plan Estratégico 2015-2019, la Agencia Española de Protección de Datos incluyó la certificación en su eje estratégico primero, relativo a la prevención para una protección más eficaz. La propia Agencia indica que «los esquemas de certificación se presentan cada vez más como herramientas útiles para conseguir en la práctica mayores niveles de protección» y prevé que una de las acciones a llevar a cabo por la misma sea la de evaluar los modelos de certificación y acreditación del cumplimiento de la normativa de protección de datos.

Pues bien, quedándonos con estas dos últimas ideas favorecedoras de la transparencia y demostrativas del cumplimiento activo de las responsabilidades legales que impone el RGPD a los responsables y encargados de tratamiento en aras de informar a los interesados del tratamiento de sus datos, nos quedamos con la idea de la confianza que se transmite al usuario. Confianza no en que no se van a tratar sus datos, sino confianza en el hecho de que sus datos se tratan conforme a las estipulaciones legales. No olvidemos que nuestro fin último es informar de la manera más completa y sencilla a los interesados con un doble objetivo. En primer lugar, que el consentimiento que presten sea realmente informado, y en segundo lugar, que se les haga conocedores del tratamiento real que se lleva a cabo de sus datos. Como este segundo planteamiento es

realmente técnico y complejo, se dota de este mecanismo en el que los usuarios depositarán su confianza.

Por otro lado, si se produce un tratamiento desleal de los datos, se traducirá en una pérdida de la valoración por parte de la entidad certificadora, disminuyendo su evaluación positiva en la calidad del tratamiento de los datos, incluso llegando a la no certificación, o bien, se traducirá en un instrumento en manos del usuario para poder reclamar la responsabilidad de los responsables y encargados del tratamiento, o incluso de la propia entidad certificadora. Este último concepto gira en torno al principio responsabilidad activa o accountability del RGPD.

En segundo lugar, el propio artículo 12 RGPD, al tratar sobre la transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado, concede en su apartado 7 la posibilidad por la cual «la información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto».

Nos debemos referir al Considerando 166 RGPD por el que se confiere la posibilidad a la Comisión para adoptar actos delegados en relación con los criterios y requisitos para los mecanismos de certificación, la información que debe presentarse mediante iconos normalizados y los procedimientos para proporcionar dichos iconos. Esta posibilidad ha sido trasladada al artículo 12.8 del mismo texto legal.

Con la combinación de estas dos nuevas medidas dotaremos a los usuarios de un instrumento potencialmente válido y suficiente para mantenerse informados respecto al tratamiento de sus datos. Por un lado, y en relación a los certificados y las evaluaciones por parte de terceros de los procedimientos llevados a cabo en el tratamiento de los datos, crearemos un código de colores que gradúen el nivel de cumplimiento por su parte. Se puede ir desde el verde si es óptimo y el tratamiento cumple con todos los requerimientos normativos, hasta el color rojo si no cumple alguno de ellos,

o lo hace de un modo no transparente. De este modo, se crearía una etiqueta con el fondo del color correspondiente al nivel de cumplimiento normativo. El usuario al identificar el color, no sabría todas las especificidades del tratamiento, pero sabría de una manera clara y directa el grado de cumplimiento. A la hora de contratar un servicio o instalar una aplicación, este conocimiento es fundamental para otorgar su consentimiento, esta vez informado, para el tratamiento.

Por supuesto, y como no todas las aplicaciones llevan a cabo los mismos tratamientos, se crearían una serie de iconos gráficos normalizados que vinieran a identificar la diferente tipología de tratamientos que se realizan por parte de los responsables o encargados del tratamiento de los datos personales.

BIBLIOGRAFÍA

Bibliografía citada

- Abad Amorón, M. R. (1993). Libertad informática y nuevos derechos: una polémica legislación. *Revista Telos*, *33*.
- Álvarez Martín, J. A. (2012). El control de los recursos públicos condición inevitable de la democracia real. Málaga: Fundación Asesores Legales.
- Álvarez Rico, M. (1979). El derecho de acceso a los documentos administrativos. *Documentación Administrativa, 183*.
- Álvarez Rigaudias, C. (2015). El poder del usuario digital. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo Derecho europeo de protección de datos* Valencia: Tirant lo Blanch.
- Andreu Martínez, M. B. y Plana Arnaldos, M. C. (2013). El poder de disposición del titular como facultad principal del derecho a la protección de los datos personales: su efectividad en el actual escenario tecnológico. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica: riesgos, amenazas y respuestas desde la perspectiva jurídica.* Navarra: Aranzadi.
- Aparicio Salom, J. (2009). Estudios sobre la Ley Orgánica de Protección de Datos de Carácter Personal. Navarra: Aranzadi.
- Barrero Rodríguez, M.C. (2014). El derecho de acceso a la información: publicidad pasiva. En Guichot Reina, E. (Coord). *Transparencia, acceso a la información pública y buen gobierno. Estudio de la Ley 19/2013*, de 9 de diciembre. Madrid: Tecnos
- Barrero Rodríguez, M.C. (2014). Publicidad Activa. En Guichot Reina, E. (Coord). *Transparencia, acceso a la información pública y buen gobierno. Estudio de la Ley 19/2013*, de 9 de diciembre. Madrid: Tecnos

– Basterra, M. I. (2006) El Derecho Fundamental de Acceso a la Información Pública. Buenos Aires: Lexis Nexis.
– Batini, C. (2010). Data Governance. En G. Viscusi, C. Batini y M. Mecella, *Information Systems for eGovernment*, Heidelber: Springer–Verlag.
– Bermejo Vera, J. (1993). La participación de los administrados en los órganos de la Administración Pública. En *La protección jurídica del ciudadano. Estudios en homenaje al profesor Jesús González Pérez, Tomo I*. Madrid: Civitas.
– Bing, J. (1990). Three Generations of Computerized Systems for Public Administration and Some Implications for Legal Decision-Making, *Ratio* Juris*, 3 Issue 2*.
– Blasco Díaz, J. L. (2010). El sentido de la transparencia administrativa y su concreción legislativa. En García Macho. R. (ed.), *Derecho administrativo dela información y administración transparente*. Madrid: Marcial Pons.
– Bovens, M. (2007). Public Accountability. En Ferlie, E., Lynn Jr. L. E. y Pollitt C. (Eds.). *The Oxford Handbook of Public Management.* Oxford: Oxford University Press.
– Carpio Cámara, M. (2016). Seguridad del tratamiento de los datos personales y notificaciones de violaciones de seguridad. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Editorial REUS.
– Čas, J. (2010). Computació́ ubicua, privacidad y protecció́ de datos: opciones y limitaciones para reconciliar contradicciones sin precedentes. *Revista Española de Protección de Datos, 6*.
– Castells, M. (1996). La era de la información. Volumen I. La sociedad red. Madrid: Alianza.
– Cavoukian A. (2009). Privacy by Design.
– Cavoukian, A. (2010). Privacy by Design The 7 Foundational Principles Implementation and Mapping of Fair Information Practices.
– Cavoukian, A. (2011). Privacy by Design. Los 7 principios fundamentales.

- Cerrillo i Martínez, A. (1998). La transparencia administrativa: Unión Europea y medio ambiente. Valencia: Tirant lo Blanch.
- Cerrillo i Martínez, A. (2000). Régimen jurídico de la información administrativa. En Tornos Mas, J. y Galán Galán, A. *La comunicación pública. La información administrativa al ciudadano*. Madrid: Marcial Pons.
- Cerrillo i Martínez, A. (2005). E-información: hacia una nueva regulación del acceso a la información. *Revista Internet, Deret i Política*.
- Cerrillo i Martínez, A. (2006). La información del sector público: del acceso a la reutilización. En Cerrillo Martínez, A. y Galán Galán, A. (Coord.), *La reutilización de la información del sector público*. Granada: Comares.
- Cotino Hueso, L. (2013). Derecho y "Gobierno Abierto", La regulación de la transparencia y la participación y su ejercicio a través del uso de las nuevas tecnologías y las redes sociales por las Administraciones Públicas. Propuestas concretas. En Bermejo Latre, J.L. y Castel Gayan, S (eds.), *Transparencia, participación ciudadana y administración pública en el siglo XXI*. Zaragoza: IAAP.
- De Palma del Teso, A. (1996) *El principio de culpabilidad en el derecho administrativo sancionador*. Madrid: Tecnos.
- Del Castillo Vázquez, I. C. (2007). Transparencia, acceso a la documentación administrativa y protección de datos de carácter personal. *Foro: Revista de ciencias jurídicas y sociales, 6*.
- Delgado Echevarría, J. (2005). La voluntad negocial y sus vicios. En Lacruz Berdejo, J. L. y otros. *Elementos de Derecho civil, Tomo I. Parte General. Volumen III*. Madrid: Dykinson
- Dembitz Brandeis, L. (1914). Other People´s Money and How the Bankers Use It.
- Dembitz Brandeis, L. y Warren S. D. (1890). The right to privacy. *Harvard Law Review, vol. IV, 5.*
- Díez Sánchez J. J. (1999). *Razones de Estado y Derecho*. Valencia: Tirant lo Blanch.

– Duaso Calés, R. (2016). Los principios de protección de datos desde el diseño y protección de datos por defecto. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus.
– Dumbill, E. (2012). Getting up to Speed with Big Data. En *Big Data Now: 2012 Edition*. Sebastopol: O´Reilly Media, Inc.
– Edwards, L. y Abel, W. (2014). The use of privacy icons and standard contract terms for generating consumer trust and confidence in digital services. CREATe Working Paper Series.
– Erbiti Zabalza, F. (2003). La comunicación: asignatura pendiente de las instituciones de control. *Auditoría Pública, 33.*
– Fernández López, J. M. (2010). Principio de consentimiento. En Troncoso Reigada, A. (dir.), *Comentario a la Ley Orgánica de Protección de Datos de Carácter Personal*, Madrid: Civitas.
– Fernández Ramos, S (1997). El derecho de acceso a los documentos administrativos. Madrid: Marcial Pons.
– Fernández Ramos, S. (2013). El acceso a la información en el Proyecto de Ley de Transparencia, acceso a la información pública y buen gobierno. Zaragoza: IAAP.
– Fernández Ramos, S. (2017). El derecho de acceso a la Información Pública en España. Navarra: Aranzadi.
– Fernández Salmerón, M. (2003) La protección de los datos personales en las Administraciones Públicas. Madrid: Civitas.
– Fernández Salmerón, M. (2006). El régimen jurídico de la reutilización comercial de la información del sector público: sujetos destinatarios y tipos de información. En Galán Galán, A. y Cerrillo i Martínez, A. (coords.): *La reutilización de la información del sector público*. Granada: Comares.
– Fernández-Samaniego, J. y Fernández-Longoria, P. (2016). El Derecho a la Portabilidad de los Datos. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus.
– Fernando Pablo, M.: (1993) *La motivación del acto administrativo*, Madrid: Tecnos.

– García de Enterría Martínez-Carande, E. (1989). Principio y modalidades de la participación ciudadana en la vida administrativa. En Gómez-Ferrer Morant, R. (coord.). *Libro homenaje al profesor José Luis Villar Palasí*. Madrid: Civitas.
– García Herrero, J. (2016). Privacidad desde el Diseño o "Privacy by Design" en el Reglamento General de Protecció de Datos (I) y (II).
– Garriga Domínguez, A. (2016). Nuevos retos para la protección de datos personales. En la Era del Big Data y de la computación ubicua. Madrid: Dykinson.
– Gay Fuentes, C. (1995). Intimidad y tratamiento de datos en las Administraciones Públicas. Madrid: Complutense.
– Gil González, E. (2016). *Big data, privacidad y protección de datos*. Madrid: Boletín Oficial del Estado.
– Guerrero Picó, M.C. (2006). El impacto de internet en el derecho fundamental a la protección de datos de carácter personal. Madrid: Civitas.
– Guichot Reina E. (2012). El Proyecto de Ley de Transparencia y acceso a la información pública y el margen de actuación de las Comunidades Autónomas. *Revista Andaluza de Administración Pública, 84*. Sevilla: IAAP.
– Guichot Reina, E. (2008). Un paso decisivo en la clasificación de las relaciones entre derecho de acceso y derecho a la protección de datos: la Sentencia del TPI de 8 de noviembre de 2007, Bavarian Lage/Comisión, t-194/04. *Revista Española de Derecho Europeo, 27*. Madrid: Civitas.
– Guichot Reina, E. (2009). *Publicidad y privacidad de la información* Administrativa. Pamplona: Aranzadi.
– Guichot Reina, E. (2011). Transparencia y acceso a la información pública en España: análisis y propuestas legislativas. *Fundación Alternativas*, *170*.
– Guichot Reina, E. (2014). Transparencia, Acceso a la Información Pública y Buen Gobierno: Estudio de la Ley 19/2013, de 9 de diciembre. Madrid: Tecnos.

– Guichot Reina. E. (2012). Transparencia versus Protección de Datos. En Blasco Esteve A. (Coord) El Derecho Público de la crisis económica. Transparencia y Sector Público. Hacia un nuevo Derecho Administrativo. Madrid: INAP.
– Guichot Reina.E. (2014). Ejercicio del derecho de acceso a la información pública y régimen de impugnaciones. En Wences, I, Kólling, M. y Ragone, S. (Coords.) *La Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno. Una perspectiva académica*. Madrid: Centro de Estudios Constitucionales y Políticos,
– Harden, I. (2001). Citizenship and Information. *European Public Law*, *vol. 7, Issue 2*. Países Bajos: Kluwer Law International.
– Heald, D. (2006). Varieties of Transparency. En Hood, C. y Heald, D. (Eds.). *Transparency. The Key to Better Governance?,* Oxford: Oxford University Press.
– Heredero Higueras, M. (1983). La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del censo de población**.** *Documentación Administrativa, 198, pp 139-159*.
– Hernández Corchete, J. A. (2016). Transparencia en la información al interesado del tratamiento de sus datos personales y en el ejercicio de sus derechos. En Piñar Mañas, J.L. *Reglamento General de Protección de Datos. Hacia un nuevo modelo europeo de Privacidad*. Madrid: Reus.
– Hunt, G. (2006). The principle of complementarity: freedom of information, public accountability and whistleblowing. En Chapman, R. A. y Hunt, M. (Eds.) *Open government in a theorical and practicas context*. Aldershot: Ashgate Publishing.
– Hustinx, P. (2010). Privacy by Design: delivering the promises. *Identity in the Information* Society, Volume 3, Issue 2. Nueva York: Springer.
– Kranenborg, H.y Voermans, W. (2005). Access to Information in the European Union. A Comparative Analysis of EC and Member State Legislation. Países Bajos: Europa Law Publishing.

- Laguna De Paz, J. C. (2010). Principio de confidencialidad. En Santamaría Pastor, J. A. (Dir.). *Los principios jurídicos del Derecho Administrativo.* Madrid: La Ley.
- Leith, Ph. (2008). Privacy as Slogan. En, Saarenpää, A. (Ed.), *Legal* privacy, Zaragoza: Prensas Universitarias.
- Lessig L. (2001). El código y otras leyes del ciberespacio, Madrid: Taurus.
- Lessig L. (2009). *Código 2.0*. Madrid: Traficantes de sueños.
- Lessig, L. (2009). Against transparency, *The New Republic.*
- Maldoff, G. (2016) The Risk-Based Approach in the GDPR: Interpretation and Implications. *IAPP*.
- Martín Rebollo, L. (1977). *La responsabilidad patrimonial de la Administración en la jurisprudencia*, Madrid: Civitas.
- Martín Rebollo, L. (2011). Fundamento y función de la responsabilidad patrimonial del Estado: situación actual y perspectivas en el derecho español. *Revista española de Derecho Administrativo*, *4*.
- Martínez Martínez, R. (2004), Una aproximación crítica a la autodeterminación informativa. Madrid: Civitas-APDCM.
- Martínez Martínez, R. (2012). Interés legítimo y protección de datos personales en la sentencia de 8 de febrero de 2012 del TS.
- Martínez Martínez, R. (2014). De la opacidad a la casa de cristal. El conflicto entre privacidad y transparencia. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.) *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Thomson-Reuters Aranzadi.
- Mayer-Schönberger, V. Y Cukier, K. (2013). *Big data: la revolución de los datos masivos*, Madrid: Turner.
- Messía de la Cerda Ballesteros, J. A. (2003). *La cesión o comunicación de datos de carácter personal*. Madrid: Thomson-Civitas-APDCM.
- Mestre Delgado, J.F. (1993). El derecho de acceso a archivos y registros administrativos [análisis del artículo 105.b) de la Constitución]. Madrid: Civitas.

– Miralles, R. (2013). El derecho a la portabilidad de los datos personales o prestación «premium» del tradicional derecho de acceso. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Pamplona: Aranzadi.
– Montilla Martos, J. L. (2016). Transparencia y acceso a la inormación en España. En Wolfgang Sarlet, I; Montilla Martos, J. A. y Linden Ruaro, R. (Coords.). Acesso à informaçâo como direito fundamental e dever estatal. Porto Alegre: Livraria do Advogado.
– Moretón Toquero, A. (2014). Los límites del derecho de acceso a la información pública. *Revista jurídica de Castilla y León, 33*.
– Mulgan, R. (2000) ”Accountability”: an ever-expanding concept?. *Public Administration, 78*, *Issue 3*.
– Mulligan, D. K. y King, J. (2012). Bridging the gap between privacy and design. *University of Pennsylvania Journal of Constitutional Law*, *14, Issue 4*.
– Muñoz Soro J.F. y Bermejo Latre, J. L. (2014). La redefinición del ámbito objetivo de la transparencia y del derecho de acceso a la información del sector público. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público. Del derecho de acceso a la reutilización de la información*, Navarra: Thomson Reuters Aranzadi.
– Murillo de la Cueva, P. L. (1990). *El derecho a la autodeterminación informativa*. Madrid: Tecnos.
– Murillo de la Cueva, P. L. (1993). Informática y protección de datos personales (Estudio sobre la Ley Orgánica 5/1992, de regulación del tratamiento automatizado de los datos de carácter personal). Madrid: Centro de Estudios Constitucionales.
– Murillo de la Cueva, P. L. (1999). La construcción del derecho a la autodeterminación informativa. *Revista de Estudios Políticos, 104.* Madrid: CEPC.
– Murillo de la Cueva, P. L. (2007). Perspectivas del derecho a la autodeterminación informativa. *IDP. Revista de Internet, Derecho y Política, 5*.

– Navas Navarro, S. (2017). La personalidad virtual del usuario de internet. Tratamiento de la información personal recogida mediante cookies y tecnología análoga. Valencia: Tirant lo Blanch.
– Oliver Lalana, A. D. y Muñoz Soro J. F. (2013). El mito del consentimiento y el fracaso del modelo individualista de protección de datos. En Valero Torrijos, J. *La protección de datos personales en internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*. Navarra: Aranzadi.
– Parejo Alfonso, L. (1996). El derecho fundamental a la intimidad y sus restricciones. En López Ortega, J. J.(Dir.). *Perfiles del derecho constitucional en la vida privada y familiar*. Madrid: Consejo General del Poder Judicial.
– Pascual García, J. (2014). Régimen jurídico del gasto público. Presupuestación, ejecución y control, Madrid: Boletín Oficial del Estado.
– Pasquier, M. y Villeneuve, J. P. (2007). Organizational barriers to transparency: a typology and analysis of organizational behavior tending to prevent or restrict access to information. *International Review of Administrative Sciences*, *73*.
– Patrick Nolan, M. (1996). Normas de conducta para la Vida Pública. *Documentos INAP, 9*.
– Piñar Mañas J. L. (2005). El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. *Asamblea: Revista Parlamentaria de la Asamblea de Madrid, 13.*
– Piñar Mañas J. L. (2009). Seguridad, transparencia y protección de datos: el futuro de un necesario e incierto equilibrio. *Fundación Alternativas, 147*.
– Piñar Mañas J. L. (2010). Concepto de dato personal. En Troncoso Reigada. A, (Dir.). *Comentario a la Ley orgánica de protección de datos de carácter personal*, Madrid: Civitas-Thomson.
– Piñar Mañas, J. L. (2010). Transparencia y protección de datos: las claves de un equilibrio necesario. En Ruiz Ojeda, A. L. (Coord.), *El gobierno local. Estudios en homenaje al profesor Luis Morell Ocaña*, Madrid: Iustel.

– Piñar Mañas, J. L. (2014). Transparencia y derecho de acceso a la información pública. Algunas reflexiones en torno al derecho de acceso en la Ley 19/2013, de transparencia, acceso a la información y buen gobierno. *Revista catalana de dret públic, 49*.
– Piñar Mañas, J. L. (2014). Transparencia y protección de datos. Una referencia a la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información y buen gobierno. En Piñar Mañas, J.L. (Coord.). *Transparencia, acceso a la información y protección de datos.* Madrid: Reus.
– Piñar Mañas, J. L. (2011). La importante reforma del régimen sancionador en materia de protección de datos: reflexiones urgentes», *Datospersonales.org: La revista de la Agencia de Protección de Datos de la Comunidad de Madrid*, *50*.
– Pitschas, R. (2006). El Derecho administrativo de la información. La regulación de la autodeterminación informativa y el gobierno electrónico», en Barnés Vázquez, J. (Coord). *Innovación y reforma en el Derecho administrativo*, Sevilla: Derecho Global.
– Pomed Sánchez, L. A. (1989). El acceso de los ciudadanos a los archivos y registros administrativos, Madrid: INAP.
– Poullet, Y. (2005). Pour une troisième generation de réglementations de protection des données. *Jusletter, 3*.
– Poullet, Y. (2008). La protection des données: un nouveau droit constitutionnel: pour une troisième génération de réglementations de protection des données. En *Droit constitutionnel et vie privée,*p. 297-365. Thunis: Académie internationale de droit constitutionnel.
– Poullet, Y. (2011). Internet et Sciences Humaines ou «Comment comprendre l'invisible?». *Revue des Questions Scientifiques*, *182, Issue 4.*
– Pulido Jiménez, M. Á. (2006). Una aproximación a la información pública en poder de la CNDH. El acceso a la información en la CNDH. En A. Ruiz Euler (Coord.), *Transparencia y Rendición de Cuentas*. México DF: Fontamara.
– Puyol Montero, J. (2015). La regulación de las medidas de seguridad. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo derecho*

europeo de protección de datos: Towards a new european data protection regime. Valencia: Tirant lo Blanch.

– Rallo Lombarte, A. (2008). What do Citizens Know and Feel? What art they fear on new tecnologies? Roma: Conferencia de Autoridades de Protección de Datos y Privacidad.
– Rallo Lombarte, A. (2014). *El derecho al olvido en Internet. España contra Google*, Madrid: Centro de Estudios Políticos y Constitucionales.
– Rallo Lombarte, A. (2014). Estudios sobre la evolución del régimen sancionador en la legislación de protección de datos. *Revista de Estudios Políticos*, *166*, 2014.
– Ramos Simón, F. (2003). La reutilización de la información del sector público. Aproximación del contenido de la propuesta de directiva 2002. *Revista General de Información y Comunicación, 13, núm. 2*.
– Rams Ramos, L. (2008). El derecho de acceso a archivos y registros administrativos. Madrid: Reus.
– Recio Gayo, M. (2015). Acerca de la evolución de la figura del encargado del tratamiento. *Revista de Privacidad y Derecho Digital*, *nº 0*.
– Rodríguez Álvarez, J.L. (2016). Transparencia y protección de datos personales: criterios legales de conciliación. En Canals i Ametller, D (Ed.). *Datos. Protección, Transparencia y Buena Regulación*. Girona. Documenta Universitaria.
– Rubí Navarrete, J. (2013). La propuesta del Reglamento General de Protección de Datos de la Unión Europea. En *Comunicaciones e propiedad industrial y derecho de la competencia, 70*.
– Rubinstein, I. (2012). Regulationg Privacy by Design, *Berkeley Technological Law Journal, 26*.
– Sáinz Moreno, F. (2004). Secreto y transparencia. En Sáinz Moreno, F. (Dir.). *Estudios para la reforma de la Administración Pública.* Madrid: INAP.
– Sáiz Peña, C. A. (2015). La notificación de brechas de seguridad. En Rallo Lombarte A; García Mahamut, R. (dir.): *Hacia un nuevo derecho europeo de protección de datos.* Valencia: Tirant lo Blanch.

– Salvador Carrasco, L. (2015). Ciber-resiliencia. Boletín electrónico del Instituto Español de Estudios Estratégicos, 35.
– Sánchez de Diego Fernández de la Riva, M. (2008). Un derecho fundamental a acceder a la información pública. *El derecho de acceso a la información pública Actas del Seminario Internacional Complutense 27 -28 junio 2007.* Madrid: CERSA.
– Schedler, A. (1999). Conceptualizing Accountability. En Schedler, A., Diamond L., y Plattner, Marc F. (Eds.). *The Self-restraining state. Power and Accountability in New Democracies*, Boulder: Lynne Rienner Publishers.
– Schwabe, J. (2009). Jurisprudencia del Tribunal Constitucional Federal Alemán. Berlín: Konrad-Adenauer-Stiftung e V.
– Serrano Pérez, M.M. (2005). El derecho fundamental a la protección de datos. Su contenido esencial. En Terol Becerra, M. J. (Dir.). *Nuevas políticas públicas: Anuario multidisciplinar para la modernización de las Administraciones Públicas*, *1*. Sevilla: IAAP.
– Solernou Viñolas, A. (2006). Los datos personales como límite a la reutilización de la información del sector público. En Cerrillo i Martínez, A. y Galán Galán, A. (Coord.): *La reutilización de la informació del sector público*. Granada: Comares.
– Sommermann, K. P. (2010). La exigencia de una Administración transparente en la perspectiva de los principios de democracia y del Estado de Derecho. En García Macho, R. (Ed.), *Derecho administrativo de la información y administración transparente*. Madrid: Marcial Pons.
– Tene, O y Polonetsky J. (2012). Privacy in the Age of Big Data. A Time for Big Decisions. *Stanford Law Review online, 63.*
– Tomás Mallén, B. (2004) El derecho fundamental a una buena administración. Madrid: INAP
– Tomás Mallén, B. (2015). Transparencia y protección de datos: nuevos desafíos para la garantía europea de los derechos fundamentales. En Rallo Lombarte, A. y García Mahamut, R. *Hacia un nuevo Derecho europeo de protección de datos*. Valencia: Tirant lo Blanch.

– Troncoso Reigada, A. (2010). *La protección de datos personales. En busca del equilibrio*. Valencia: Tirant Lo Blanch.
– Troncoso Reigada, A. (2012). Hacia un nuevo marco jurídico europeo de la protección de datos personales. *Revista Española de Derecho Europeo, 43*.
– Valero Torrijos, J. (2012). El acceso y la reutilización de la información administrativa. Implicaciones jurídicas del proceso de modernización tecnológica de las Administraciones Públicas en su actual y futura configuración», *Diario La Ley*, *7800*.
– Valero Torrijos, J. (2013). *Derecho, innovación y Administración electrónica*. Sevilla: Derecho Global.
– Valero Torrijos, J. (2013). Las quiebras en Internet de la regulación legal del derecho a la protección de los datos de carácter personal: la necesaria superación de un modelo desfasado. En Valero Torrijos, J. (Coord..). *La protección de los datos personales en Internet ante la innovación tecnológica. Riesgos, amenazas y respuestas desde la perspectiva jurídica*, Navarra: Aranzadi.
– Valero Torrijos, J. (2014). Acceso, reutilización y gestión avanzada de la información en el ámbito de la administración sanitaria. Implicaciones jurídicas desde la perspectiva de la innovación tecnológica. En Valero Torrijos, J. y Fernández Salmerón, M. (Coords.). *Régimen jurídico de la transparencia del sector público: del Derecho de acceso a la reutilización de la información*. Navarra: Aranzadi.
– Villaverde Menéndez, I (1995). *Los derechos del público*. Madrid: Tecnos.
– Warren, A.; Bayley, R.; Bennett, C.; Charlesworth, A. J.; Clarke, R.; y Oppenheim, C. (2009). Privacy Impact Assessments: The UK Experience 31st International Conference of Data Protection and Privacy Commissioners.
– Weiser, M. (1991). The Computer for the 21st Century. *Scientific American.*

– Whitley, E.A. y Kanellopoulou, N. (2010). Privacy and informed consent in online interactions: Evidence from expert focus groups. *Association for Information Systems. ICIS 2010 Proccedings.*

Legislación Española

– Constitución Española. BOE núm. 311, de 29 de diciembre de 1978.
– Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. «BOE» núm. 17, de 19/01/2008.
– Real Decreto 415/2016, de 3 de noviembre, por el que se reestructuran los departamentos ministeriales. BOE núm 267, de 4 de noviembre de 2016.
– Real Decreto-ley 13/2012, de 30 de marzo, por el que se transponen directivas en materia de mercados interiores de electricidad y gas y en materia de comunicaciones electrónicas, y por el que se adoptan medidas para la corrección de las desviaciones por desajustes entre los costes e ingresos de los sectores eléctrico y gasista. Boletín Oficial del Estado nº 78, de 31 de marzo de 2012.
– Ley 16/1985, de 25 de junio, del Patrimonio Histórico Español. BOE núm 155, de 29/06/1985.
– Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. BOE núm 276, de 17 de noviembre de 2007.
– Ley 18/2015, de 9 de julio, por la que se modifica la Ley 37/2007, de 16 de noviembre, sobre reutilización de la información del sector público. BOE núm, 164, de 10 de julio de 2015.
– Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno y el resto del Ordenamiento Jurídico.
– Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico, BOE núm 166, de 12/07/2002.

– Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. BOE núm. 236, de 2 de octubre de 2015.
– Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. BOE» núm. 236, de 02/10/2015.
– Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, BOE núm 114, de 10/05/2014.
– Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común. BOE núm 285, de 27/11/1992.
– Ley Orgánica 5/1992, de 29 de octubre, de Regulación del Tratamiento Automatizado de los Datos de Carácter Personal. (BOE de 31 de octubre de 1992. LORTAD)
– Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. BOE núm 298, de 14/12/1999.

Legislación Europea

– Carta de los Derechos Fundamentales de la Unión Europea DOCE C 364, de 18de diciembre de 2000.
– Comisión de las Comunidades Europeas. (2003). Primer informe sobre la aplicación de la Directiva sobre protección de datos (95/46 CE). [COM (2003) 265 final], de 15 de mayo de 2003.
– Comisión de las Comunidades Europeas. (2008). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión. COM (2008) 229 final, de 30 de abril de 2008.
– Comisión Europea (2001) eEUROPE 2002: creación de un marco comunitario para la explotación de la información del sector público. Comunicación de la Comisión al Consejo, el Parlamento Europeo, el Comité Económico y Social y el Comité de las Regiones COM (2001) 607 final, de 23 de octubre de 2001.
– Comisión Europea. (2012). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas

en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos). COM (2012) 11 final, de 25 de enero de 2012.

– Comisión Europea. (2016). Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se establece el Código Europeo de las Comunicaciones Electrónicas (Refundición) COM (2016) 590 final, de 12 de octubre de 2016.
– Comisión Europea. (2017). Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión y a la libre circulación de estos datos, y por el que se deroga el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE. COM (2017) 08 final, de 10 de enero de 2017.
– Comisión Europea. (2017). Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE (Reglamento sobre la privacidad y las comunicaciones electrónicas) COM (2017) 10 final, de 10 de enero de 2017.
– Comunicación de la Comisión al Consejo, el Parlamento Europeo, el Comité Económico y Social y el Comité de las Regiones. La eEUROPE 2002: creación de un marco comunitario para la explotación de la información del sector público. COM (2001) 607 final, de 23 de octubre de 2001.
– Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre el fomento de la protección de datos mediante las tecnologías de protección del derecho a la intimidad (PET) COM (2007) 228 final, de 2 de mayo de 2007.
– Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones. Un enfoque global de la protección de los datos personales en la Unión Europea COM (2010) 609 final.

– Comunicación de la Comisión sobre la protección de las personas en lo referente al tratamiento de datos personales en la Comunidad y a la seguridad de los sistemas de información; Propuesta de Directiva del Consejo relativa a la protección de las personas en lo referente al tratamiento de datos personales. COM (90) 314 final.
– Consejo de la Unión Europea, Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) - Preparación de un planteamiento general, 11 de junio de 2015.
– Consejo de la Unión Europea. (2015) Propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), preparación de un planteamiento general, documento del Consejo 9565/15, de 11 de junio de 2015.
– Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos. Tromsø, 18 de junio de 2009.
– Decisión 93/731/CE DOCE L 340, de 31 de diciembre de 1993.
– Decisión del Consejo 93/731/CE, de 20 de diciembre de 1993, relativa al acceso del público a los documentos del Consejo, DOCE L-340 de 31/12/1993.
– Decisión del Consejo, de 20 de mayo de 1996, por la que se adopta un Programa plurianual de la Comunidad para fomentar el desarrollo de la industria europea de los contenidos multimedios y la utilización de éstos en la naciente sociedad de la información (INFA 2000) DOCE L 129, de 30 de mayo de 1996.
– Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo de 6 de julio de 2016 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. DOUE L194, 19 de julio de 2016.
– Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la

protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) DOCE L 201, de 31 de julio de 2002.

– Directiva 2003/98/CE del Parlamento Europeo y del Consejo de 17 de noviembre de 2003 relativa a la reutilización de la información del sector público. DOUE L345, de 31de diciembre de 2003.
– Directiva 2009/136/CE del Parlamento Europeo y del Consejo, de 25 de noviembre de 2009 , por la que se modifican la Directiva 2002/22/CE relativa al servicio universal y los derechos de los usuarios en relación con las redes y los servicios de comunicaciones electrónicas, la Directiva 2002/58/CE relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas y el Reglamento (CE) n o 2006/2004 sobre la cooperación en materia de protección de los consumidores. DOUE L 337, de 18 de diciembre de 2009.
– Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público. DOUE núm 175, de 27 de junio de 2013.
– Directiva 2015/1535 del Parlamento Europeo y del Consejo de 9 de septiembre de 2015 por la que se establece un procedimiento de información en materia de reglamentaciones técnicas y de reglas relativas a los servicios de la sociedad de la información (versión codificada). DOUE L 241, 17 de septiembre de 2015.
– Directiva 90/313/CEE del Consejo, de 7 de junio de 1990, sobre libertad de acceso a la información en materia de medio ambiente Diario Oficial núm L 158, de 23 de junio de 1990.
– Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos DOCE L 281 de 23 de noviembre de 1995.
– I Informe sobre sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión

(versión refundida) (COM(2008)0229 – C7-0184/2008 – 2008/0090(COD)).

– Parlamento Europeo. (2013). Proyecto de Resolución legislativa del Parlamento Europeo sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) Comisión de Libertades Civiles, Justicia y Asuntos de Interior, de 21 de noviembre de 2013.
– Reglamento (CE) n° 1049/2001 del Parlamento Europeo y del Consejo, de 30 de mayo de 2001, relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión DO L 145, de 31 de 05 de 2001.
– Reglamento (CE) nº 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos DO L 8, de doce de enero de 2001.
– Reglamento 611/2013 de la Comisión, de 24 de junio de 2013, relativo a las medidas aplicables a la notificación de casos de violación de datos personales en el marco de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo sobre la privacidad y las comunicaciones electrónicas. DOUE L 173, de 26 de junio de 2013.
– Resolución legislativa del Parlamento Europeo, de 12 de marzo de 2014, sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))
– Tratado de Funcionamiento de la Unión Europea». DOUE núm. C 326 de 26/10/2012 p. 0013 - 0045 (Versión consolidada).

Legislación Norteamericana

- The Admisnitrative Procedure Act – 5 USC Subchapter II.
- The E-Government Act.
- The Federal Advisory Committe Act – 5 USC Appendix 2
- The Freedom of Information Act.
- The Government in the Sunshine Act of 1976 – 5 U.S.C. § 552b.
- The Privacy Act of 1974, 5 U.S.C. § 552a.

Jurisprudencia

- Sentencia Audiencia Nacional de 25 de febrero de 2013 (Sala de lo Contencioso-Administrativo, Sección 1ª)
- Sentencia Corte Interamericana de Derechos Humanos, Claude Reyes y otros c. Chile, de 19 de septiembre de 2006.
- Sentencia Tribunal Constitucional 158/2009, de 25 de junio.
- Sentencia Tribunal Constitucional 17/2013, de 31 de enero de 2013.
- Sentencia Tribunal Constitucional 254/1993, de 20 de julio de 1993.
- Sentencia Tribunal Constitucional 292/2000, de 30 de noviembre de 2000.
- Sentencia Tribunal Constitucional 96/2012, de 7 de mayo de 2012.
- Sentencia Tribunal Constitucional Federal de Alemania, de 15 de diciembre de 1983.
- Sentencia Tribunal de Justica (Gran Sala) de 1 de julio de 2008, Reino de Suecia y Maurizio Turco contra Consejo de la Unión Europea, asuntos acumulados C- 39/05 P y C-52/05 P.
- Sentencia Tribunal de Justica (Gran Sala) de 9 de noviembre de 2010, Volker und Markus Schecke y Hartmut Eifert, asuntos acumulados C- 92/09 y C-93/09.
- Sentencia Tribunal de Justicia (Gran Sala) de 26 de enero de 2010, Internationaler Hilfsfonds contra Comisión Europea, asunto C-362/08 P.
- Sentencia Tribunal de Justicia (Gran Sala) de 26 de enero de 2010 (caso Internationaler Hilfsfonds contra Comisión Europea)

- Sentencia Tribunal de Justicia (Gran Sala) de 30 de mayo de 2006, Parlamento Europeo c. Consejo de la Unión Europea C-317/04 y Comisión de las Comunidades Europeas C-318/04.
- Sentencia Tribunal de Justicia (Gran Sala) de 5 de octubre de 2004, Pfeiffer Roith, Süß, Winter, Nestvogel, Zeller, Döbele, en los asuntos acumulados C-397/01 a C-403/01.
- Sentencia Tribunal de Justicia de 12 de diciembre de 2013, petición de decisión prejudicial planteada por el Gerechtshof te ´s-Hertogenbosch, asunto C-486/12.
- Sentencia Tribunal de Justicia de 7 de mayo de 2009, College van burgemeester en wethouders van Rotterdam c. M.E.E. Rijkeboer, asunto C-553/07.
- Sentencia Tribunal de Justicia de la Unión Europea de 16 de julio de 2015, asunto C-615/13 P. Client Earth y PAN Europe contra EFSA, Comisión Europea y el Supervisor Europeo de Protección de Datos (SEPD).
- Sentencia Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) (C-468/10) y Federación de Comercio Electrónico y Marketing Directo (FECEMD) (C-469/10) contra Administración del Estado.
- Sentencia Tribunal de Justicia de la Unión Europea de 29 de junio de 2010, asunto C-28/08 P, Comisión contra Bavarian Lager.
- Sentencia Tribunal de Justicia de la Unión Europea Strack/Comisión, C-127/13 P, EU:C:2014:2250, apartados 107 y 108;
- Sentencia Tribunal de Justicia de la Unión Europea Volker und Markus Schecke y Eifert, C-92/09 y C-93/09.
- Sentencia Tribunal de Justicia de la Unión Europea, de 16 de julio de 2015, ClientEarth/PAN Europe contra EFSA y Comisión, asunto C-615/13 P
- Sentencia Tribunal de Justicia de las Comunidades Europeas de 14 de septiembre de 2000, Asunto C-369/98, Fischer
- Sentencia Tribunal de Justicia de las Comunidades Europeas de 18 de noviembre de 1999, Asunto C-209/97, Comisión contra Consejo.

– Sentencia Tribunal de Justicia de las Comunidades Europeas de 20 de mayo de 2003, Asuntos acumulados C-465/00, C-138 y 139/01, Österreichischer Rundfunk.
– Sentencia Tribunal de Justicia de las Comunidades Europeas de 6 de diciembre de 2001, asunto C-353/99 P, Consejo c. Hautala.
– Sentencia Tribunal de Justicia de las Comunidades Europeas, Caso Lindqvist. Sentencia de 6 de noviembre de 2003.
– Sentencia Tribunal de Justicia de las Comunidades Europeas, Consejo de la Unión c. Hautala, de 6 de diciembre de 2001, asunto C-353/99 P.
– Sentencia Tribunal de Primera Instancia (Sala Quinta ampliada), de 30 de noviembre de 2004, IFAW Internationaler Tierschutz-Fonds gGmbH contra Comisión, asunto T-168/02
– Sentencia Tribunal de Primera Instancia (Sala Segunda) de 19 de enero de 2010, Co-Frutta Soc. coop. Contra Comisión Europea, asuntos acumulados T-355/04 y T-446/04.
– Sentencia Tribunal de Primera Instancia (Sala Segunda) de 19 de enero de 2010 (caso Co-Frutta Soc. coop. Contra Comisión Europea),
– Sentencia Tribunal de Primera Instancia de 8 de noviembre de 2007, Bavarian Lager contra Comisión, Asunto T-194/04.
– Sentencia Tribunal de Primera Instancia Svenska Journalistförbundet v. Council, T-174/95, ECR (1998). P. II-2289.
– Sentencia Tribunal Europeo Derechos Humanos Gaskin c. The United Kingdom, de 07 de julio de 1989.
– Sentencia Tribunal Europeo Derechos Humanos Kennedy c. Hungría, de 16 de agosto de 2009.
– Sentencia Tribunal Europeo Derechos Humanos Loiseau c. Francia, de 28 de septiembre de 2004.
– Sentencia Tribunal Europeo Derechos Humanos Sdruzeni Jihoceské Matky c. República Checa, de 10 de julio de 2006.
– Sentencia Tribunal Europeo Derechos Humanos Társasag a Szabadságjogokert c. Hungría, de 14 de abril de 2009.
– Sentencia Tribunal Supremo de 19 de junio de 2012.
– Sentencia Tribunal Supremo de 19 de mayo de 2003.

– Sentencia Tribunal Supremo de 30 de enero de 1989.
– Sentencia Tribunal Supremo de 30 de marzo de 1999.
– Sentencia Tribunal Supremo de 8 de febrero de 2012.
– Sentencia Tribunal Supremo de los Estados Unidos de 26 de enero de 1978, Houchins vs. KQED, 438 U.S. 1, 98 S.CR. 2588
– Sentencia Tribunal Supremo de los Estados Unidos, National Archives and Records admin. vs. Favish, [541 US 157 (2004)].
– Sentencia Tribunal Supremo de los Estados Unidos, United States Deportment of Justica v. Reporters Committee for Freedom of the Press [489 United States 749 (1989)].
– Sentencia Tribunal Supremo de los Estados Unidos. United States Department of Defense v. Federal Labor Relations Authority, [510 U. S. 487, (1994)].

Grupo de Trabajo del Artículo 29

– Grupo de Trabajo del Artículo 29. Dictamen 01/2012 sobre las propuestas de reforma de la protección de datos, WP 191, de 23 de marzo de 2012.
– Grupo de Trabajo del Artículo 29. Dictamen 10/2004 sobre una mayor armonización de las disposiciones relativas a la información, WP100, de 25 de noviembre de 2004.
– Grupo de Trabajo del Artículo 29. Dictamen 15/2011 sobre la definición del consentimiento, de 13 de julio de 2011, WP187.
– Grupo de Trabajo del Artículo 29. Dictamen 16/2011 sobre la recomendación de mejores prácticas de EASA/IAB sobre publicidad comportamental en línea, de 8 de diciembre de 2011. GT188.
– Grupo de Trabajo del Artículo 29. Dictamen 2/2009 sobre la protección de los datos personales de los niños (Directrices generales y especial referencia a las escuelas). WP 160.
– Grupo de Trabajo del Artículo 29. Dictamen 2/2010 sobre publicidad comportamental en línea, adoptado el 22 de junio de 2010 (WP 171).
– Grupo de Trabajo del Artículo 29. Dictamen 3/2012 sobre el principio de responsabilidad, de 13 de julio de 2010. GT173

– Grupo de Trabajo del Artículo 29. Dictamen 3/99 relativo a Información del sector público y protección de datos personales. Contribución a la consulta iniciada con el Libro Verde de la Comisión Europea titulado "La información del sector público: un recurso clave para Europa" COM(1998) 585, WP20, de 3 de mayo de 1999.
– Grupo de Trabajo del Artículo 29. Dictamen 4/2007 sobre el concepto de datos personales, de 20 de junio. WP 136.
– Grupo de Trabajo del Artículo 29. Dictamen 4/2012 sobre la exención del requisito de consentimiento de cookies, adoptado el 7 de junio de 2012 (WP 194).
– Grupo de Trabajo del Artículo 29. Dictamen 4/2013 sobre el modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente preparado por el Grupo de expertos 2 del Grupo especial sobre redes inteligentes de la Comisión, de 22 de abril de 2013, WP205
– Grupo de Trabajo del Artículo 29. Dictamen 5/2014 sobre técnicas de anonimización, de 10 de abril. WP 216.
– Grupo de Trabajo del Artículo 29. Dictamen 6/2014 sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la Directiva 95/46/CE. WP217, de 9 de abril de 2014.
– Grupo de Trabajo del Artículo 29. Dictamen 8/2001 sobre el tratamiento de datos personales en el contexto laboral, de 13 de septiembre de 2001 WP48
– Grupo de Trabajo del Artículo 29. Dictamen Statement on the role of a risk-based approach in data protection legal frameworks, WP 218, de 30 de mayo de 2014.
– Grupo de Trabajo del Artículo 29. Documento de trabajo sobre el tratamiento de datos personales relativos a la salud en los historiales médicos electrónicos (HME), de 15 de febrero de 2007. WP131
– Grupo de Trabajo del Artículo 29. El futuro de la privacidad: contribución común a la consulta de la Comisión Europea sobre el marco jurídico para el derecho fundamental a la protección de los datos de carácter personal», 1 de diciembre de 2009, WP 168.

– Grupo de Trabajo del Artículo 29. Recomendación 1/99 sobre el tratamiento invisible y automático de datos personales en Internet efectuado por software y hardware, de 23 de febrero de 1999.

Informes y Recomendaciones

– Agencia Española de Protección de Datos (2012) Informe al Anteproyecto de Ley de Transparencia, acceso a la información pública y buen gobierno. En
– Agencia Española de Protección de Datos (2014) Informe al Anteproyecto de Real Decreto por el se aprueba el reglamento de desarrollo de la Ley de 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, de 7 de noviembre de 2014.
– Consejo de Estado (2012). Informe 707/2012 al Anteproyecto de Ley de Transparencia, acceso a la información pública y buen gobierno, de 19 de julio de 2012.
– Consejo de Estado. Anteproyecto de Ley de transparencia, acceso a la información pública y buen gobierno, de 19 de julio de 2012.
– Consejo de Transparencia «Informe de 23 de marzo de 2015»
– Consejo de Transparencia Criterio interpretativo 2/2015, de 24 de junio de 2015.
– Dictamen 5/2001, sobre el Informe Especial del Defensor del Pueblo Europeo al Parlamento Europeo a raíz del proyecto de Recomendación dirigido a la Comisión Europea en la reclamación 713/98/IJH, de 17 de mayo de 2001.
– Dictamen del Supervisor Europeo de Protección de Datos sobre la propuesta de Reglamento del Parlamento Europeo y del Consejo relativo al acceso del público a los documentos del Parlamento Europeo, del Consejo y de la Comisión (DOUE 2009/C 07/01/2009).

– Federal Trade Commission (2009). Data Protection Accountability: The Essential Elements. A Document for Discussion. The Centre for Information Policy Leadership.
– Federal Trade Commission (2012). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers. FTC Report.
– Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC (2012) 72 final, 25 de enero de 2012.
– Information and Privacy Commissioner/Ontario y Netherlands, Registratiekamer. (1995) Privacy-enhancing technologies: the path to anonymity, Volume 1. Toronto: Information & Privacy Commissioner/Ontario.
– Information Commissioner´s Office (2011). Privacy Impact Assessment Handbook. Version 2.0. Cheshire: Information Commissioner´s Office.
– Informes de la Agencia Española de Protección de Datos (2008-0240); (2016-0005); (2012-0382); (2010-0355); (2010-0242); (2010-0162); (2011-0223); (2005-0304); (2011-0029); (2005-0304); (2011-0029).
– La información del sector público: un recurso clave para Europa. Libro verde sobre la información del sector público en la sociedad de la información. COM(1998) 585.
– Libro Blanco de 2001 sobre «La gobernanza europea» COM (2001) 428 final.
– Libro Verde «Iniciativa europea a favor de la transparencia» COM (2006) 194 final

– OCDE (2013). The OECD Privacy Guidelines.
– OCDE. (1980) Directrices de protección de datos y circulación transfronteriza de datos personales, 23 de septiembre de 1980.
– Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia. (2012) : Getting Accountability Right with a Privacy Management Program.
– Recomendación 2003/361/CE de la Comisión, de 6 de mayo de 2003, sobre la definición de microempresas, pequeñas y medianas empresas (DO L 124 de veinte de mayo de 2003).
– Recomendación de la Comisión, de 10 de octubre de 2014 relativa al modelo de evaluación del impacto sobre la protección de datos para redes inteligentes y para sistemas de contador inteligente. DOUE L 300 de 18 de octubre de 2014.
– Recomendación de la Comisión, de 9 de marzo de 2012, relativa a los preparativos para el despliegue de los sistemas de contador inteligente DOUE L73 de 13 de marzo de 2012.
– Recomendación del Consejo de Ministros del Consejo de Europa Rec (2010) 13, de 23 de noviembre de 2010, sobre la protección de las personas en relación con el procesamiento automatizado de datos personales para la creación de perfiles.
– Supervisor Europeo de Protección de Datos (2005) Public access to documents and data protection. Background Paper Series, 1.
– Supervisor Europeo de Protección de Datos (2011). Public Access to documents containing personal data after the Bavarian Lager ruling.
– Supervisor Europeo de Protección de Datos. (2011) Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions - "A comprehensive approach on personal data protection in the European Union", 14 de enero de 2011.
– United States General Accounting Office. (2001). Informe Electronic Government: Challenges must be Addressed with Effective Leadership and Management, de 11 de julio de 2001.

Otra documentación

- Agencia Española de Protección de Datos (1998). Instrucción 1/1998, de 19 de enero de 1998.
- Agencia Española de Protección de Datos (2014). Guía para una Evaluación de Impacto en la de Protección Datos Personales.
- Agencia Española de Protección de Datos (2014). Resolución R/02990/2013, de 14 de enero de 2014.
- Agencia Española de Protección de Datos (2016). El Reglamento de Protección de Datos en 12 preguntas.
- Agencia Española de Protección de Datos. (2009). Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal «Resolución de Madrid».
- Agencia Vasca de Protección de Datos. (2008). Percepciones y actitudes sobre la protección de datos personales. Vitoria: Gobierno Vasco.
- BEUC, the European Consumers' Organisation. A comprehensive approach on personal data protection in the European Union. European Commission's Communication BEUC, The European Consumers' Organisation's response, 24 de enero de 2011.
- Commission de la Protection de la vie Privée, Avis n° 35/2012 du 21 novembre 2012 d'initiative sur la proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données1 (CO-A-2012-015), Belgique.
- Commission Staff Working Paper Impact Assessment Accompanying the document Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes

of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. SEC(2012) 72 final, de 25 de enero de 2012.
– Committee on Standards in Public Life (1995). The 7 principles of public life.
– Directrices para mejorar la sinergia entre los sectores público y privado en el mercado de la información. Oficina de Publicaciones de las Comunidades Europeas. Bruselas. 1989.
– Parlamento Europeo (2016). Fichas técnicas sobre la Unión Europea.
– Resolución sobre Privacidad desde el Diseño (2010). XXXII Conferencia Internacional de Autoridades de Protección de Datos, de 27-29 de octubre de 2010.
– Verizon. (2017). Data Breach Investigations Report.